Available online at www.sciencedirect.com
ScienceDirect
Discrete Applied Mathematics 156 (2008) 3072–3090
DISCRETE APPLIED MATHEMATICS
www.elsevier.com/locate/dam

On the cycling operation in braid groups

Juan González-Meneses[a,*], Volker Gebhardt[b]

[a] *Dept. Álgebra, Facultad de Matemáticas, Universidad de Sevilla, Apdo. 1160, 41080 Sevilla, Spain*
[b] *School of Computing and Mathematics, University of Western Sydney, Locked Bag 1797, Penrith South DC NSW 1797, Australia*

Received 20 March 2007; received in revised form 2 October 2007; accepted 7 January 2008
Available online 6 March 2008

Abstract

The cycling operation is a special kind of conjugation that can be applied to elements in Artin's braid groups, in order to reduce their length. It is a key ingredient of the usual solutions to the conjugacy problem in braid groups. In their seminal paper on braid-cryptography, Ko, Lee et al. proposed the *cycling problem* as a hard problem in braid groups that could be interesting for cryptography. In this paper we give a polynomial solution to that problem, mainly by showing that cycling is surjective, and using a result by Maffre which shows that pre-images under cycling can be computed fast. This result also holds in every Artin–Tits group of spherical type, endowed with the Artin Garside structure.

On the other hand, the conjugacy search problem in braid groups is usually solved by computing some finite sets called (left) *ultra summit sets* (left-USSs), using left normal forms of braids. But one can equally use right normal forms and compute right-USSs. Hard instances of the conjugacy search problem correspond to elements having big (left and right) USSs. One may think that even if some element has a big left-USS, it could possibly have a small right-USS. We show that this is not the case in the important particular case of *rigid* braids. More precisely, we show that the left-USS and the right-USS of a given rigid braid determine isomorphic graphs, with the arrows reversed, the isomorphism being defined using iterated cycling. We conjecture that the same is true for every element, not necessarily rigid, in braid groups and Artin–Tits groups of spherical type.

Keywords: Braid groups; Garside groups; Conjugacy problem; Conjugacy search problem; Cycling; Ultra summit set; Braid-based cryptography

1. Introduction

Braid groups [3] were related to cryptography in two independent seminal papers [2,21]. In both papers, the security of the proposed cryptosystems relied on the presumed difficulty of some problems in non-commutative groups, namely the conjugacy search problem (CSP) and the multiple simultaneous conjugacy problem (MSCP). The papers proposed Artin braid groups as good candidates to implement these cryptosystems, and a lot of literature has been produced on this subject since then; see for example [13] for a survey. The results in this paper refer to braid groups as the main example, but some of them also hold in other instances of so-called *Garside groups* [11,12]. Garside groups are a family of groups sharing some basic algebraic properties with braid groups, which in particular contains all Artin–Tits groups of spherical type.

* Corresponding author. Tel.: +34 954 55 7195; fax: +34 954 55 6938.
E-mail addresses: meneses@us.es (J. González-Meneses), v.gebhardt@uws.edu.au (V. Gebhardt).
URL: http://www.personal.us.es/meneses (J. González-Meneses).

0166-218X/$ - see front matter
doi:10.1016/j.dam.2008.01.023

It seems clear that the main objection to the above cryptosystems, either in braid groups or in other groups, is the choice of keys. If one just chooses public and secret keys at random in a braid group, with given parameters such as length or number of strands, none of the above cryptosystems can be considered to be secure. It is hence crucial to be able to choose hard instances that resist all known attacks.

There are other presumably hard problems in braid groups that have been proposed as being possibly interesting for cryptography. In [21], the *cycling problem*, among others, was suggested. It can be explained as follows. In braid groups one has a well-known *left normal form*, that is, a unique way to write a braid on n strands $x \in B_n$ as a product $x = \Delta^p x_1 \cdots x_r$, where Δ is the Garside element, the half-twist, and each x_i is a simple braid. This normal form will be explicitly defined later. If we define the **initial factor** of x as $\iota_L(x) = \Delta^p x_1 \Delta^{-p}$ for $r > 0$, and $\iota_L(x) = 1$ for $r = 0$, then one has $x = \iota_L(x)\, \Delta^p x_2 \cdots x_r$. The **left cycling** of x is defined to be the conjugate of x by its initial factor. That is, $\mathbf{c}_L(x) = \Delta^p x_2 \cdots x_r\, \iota_L(x)$. The same definition makes sense in every Garside group.

The **cycling problem** asks, given an element y and a positive integer t such that y is in the image of $\mathbf{c}_L^t$, to find an element x such that $\mathbf{c}_L^t(x) = y$.

In this paper we will show that the cycling problem has a polynomial solution. Namely, it was shown in [24] that the cycling problem for $t = 1$ has a very efficient solution. That is, if y is the cycling of some element, then one can find x such that $\mathbf{c}_L(x) = y$ very fast. In the first part of this paper we will show the following result, which holds for all Garside groups satisfying some additional condition. In particular, it holds in every Artin–Tits group of spherical type (which in particular includes the braid groups) endowed with the Artin Garside structure.

Theorem 1.1. *If G is a Garside group which is atom-friendly (on the left), then $\mathbf{c}_L : G \to G$ is surjective.*

As an immediate corollary, a solution to the cycling problem is just given by applying t times the algorithm in [24]. This clearly gives a polynomial solution to the cycling problem, since the algorithm for $t = 1$ given in [24] is polynomial.

The proof of Theorem 1.1 makes use not only of left normal forms, but also of *right normal forms* of elements. We shall see that, under certain conditions, a pre-image of x under cycling, defined using left normal forms, is precisely the "cycling" of x defined using right normal forms. This shows that *left* and *right cyclings*, $\mathbf{c}_L$ and $\mathbf{c}_R$, are closely related.

In the context of the conjugacy problem in B_n, the cycling operation is mainly used to find simpler conjugates of a braid, and also to compute finite sets which are invariants of conjugacy classes and allow us to solve the conjugacy problem. One such set is the ultra summit set $\mathrm{USS}(x)$ of a given braid x. One usually defines this set by using left normal forms, but it is equally possible to define it using right normal forms, hence one actually has two finite sets associated to x, which we denote by $\mathrm{USS}_L(x)$ and $\mathrm{USS}_R(x)$.

The algorithmic solution to the conjugacy search problem in braid groups (and in any Garside group) developed in [18] relies on computing ultra summit sets. Hence, braids having small ultra summit sets are not hard instances for the conjugacy search problem. This means that if one wants to find a good key for a cryptographic protocol, one needs to choose a braid with a large ultra summit set. But we have seen that there are two kinds of ultra summit sets, $\mathrm{USS}_L(x)$ and $\mathrm{USS}_R(x)$, so the question arises of whether one of them can be large while the other one is small.

On the other hand, there are three geometric kinds of braids: periodic, reducible and pseudo-Anosov [10]. The conjugacy search problem for periodic braids is solvable in polynomial time [8]. Reducible braids are those which can be decomposed, in some sense, into braids with fewer strands. There are algorithms to find this decomposition [4], see also [23], although they are not polynomial. Nevertheless, in most cases the decomposition can be found very fast, and the conjugacy problem is split into several conjugacy problems on fewer strands. Hence, it would be desirable to know pseudo-Anosov braids whose ultra summit sets are large.

One can solve the conjugacy search problem for pseudo-Anosov braids using *rigid* braids (these will be defined later): It is shown in [19] that the conjugacy search problem for two pseudo-Anosov braids x and y is equivalent to the same problem for x^m and y^m, for every non-zero integer m. Moreover, in [6] it is shown that every pseudo-Anosov element which is contained in its ultra summit set, has a small power which is rigid (we will be more explicit in the next section). Therefore, one just needs to care about rigid braids. So the above question is transformed into the following: if x is a rigid braid, is it possible that $\mathrm{USS}_L(x)$ is large and $\mathrm{USS}_R(x)$ is small, or vice versa? The answer is negative, and it is given by the following results.

Theorem 1.2. *Let $x \in B_n$ such that $y \in \mathrm{SSS}(x)$ is a braid with canonical length $\ell(y) > 1$. Then x is conjugate to a left rigid braid if and only if it is conjugate to a right rigid braid.*

In the above case, we will show that we have $\#(\mathrm{USS}_L(x)) = \#(\mathrm{USS}_R(x))$. Moreover, if the canonical length of $y \in \mathrm{SSS}(x)$ is equal to 1, we also have $\#(\mathrm{USS}_R(x)) = \#(\mathrm{USS}_L(x))$, since cycling of elements of canonical length 1 is trivial, whence $\mathrm{USS}_L(x) = \mathrm{SSS}(x) = \mathrm{USS}_R(x)$. (As y is assumed to be rigid, we have $\ell(y) > 0$ by definition.) Therefore, if one is able to find a rigid braid x such that $\mathrm{USS}_L(x)$ is large, the same is true for $\mathrm{USS}_R(x)$, so the conjugacy search problem will be equally difficult, regardless of whether one uses left or right normal forms.

Moreover, we will show that the relation between $\mathrm{USS}_L(x)$ and $\mathrm{USS}_R(x)$ is deeper than just both having the same number of elements. In order to compute $\mathrm{USS}_L(x)$ using the algorithm in [18], one actually computes a directed graph, which we will denote by $\mathrm{USG}_L(x)$ (left ultra summit graph of x). The vertices of $\mathrm{USG}_L(x)$ correspond to the elements of $\mathrm{USS}_L(x)$ and the arrows are labelled by simple braids, in such a way that there is an arrow labelled by s going from u to v, if and only if $s^{-1}us = v$. In the same way, one can define $\mathrm{USG}_R(x)$, where in this case the vertices correspond to elements in $\mathrm{USS}_R(x)$ and there is an arrow labelled by s going from u to v, if and only if $sus^{-1} = v$. We will denote by $\mathrm{USG}_R(x)^{op}$ the directed graph which is isomorphic to $\mathrm{USG}_R(x)$ as a (non-directed) graph, but with the arrows reversed. The result that compares the graphs $\mathrm{USG}_L(x)$ and $\mathrm{USG}_R(x)$ is the following:

Theorem 1.3. *Let $x \in B_n$ be conjugate to a left rigid braid y with canonical length $\ell(y) > 1$. Then $\mathrm{USG}_L(x)$ and $\mathrm{USG}_R(x)^{op}$ are isomorphic directed graphs.*

Remark 1.4. We recently learnt from Jean Michel, François Digne and David Bessis, that $\mathrm{USG}_L(x)$ (and thus $\mathrm{USG}_R(x)$) are Garside categories. In this context, the notation $\mathrm{USG}_R(x)^{op}$ makes sense, since it refers to the opposite category. In this language Theorem 1.3 says that $\mathrm{USG}_L(x)$ and $\mathrm{USG}_R(x)^{op}$ are isomorphic Garside categories. In other words, there exists a contravariant isomorphism from $\mathrm{USG}_L(x)$ to $\mathrm{USG}_R(x)$.

This paper is structured as follows: In Section 2 some basic notions of braids and Garside theory are recalled. Specialists in Garside theory may skip this section and go directly to Section 3, in which Theorem 1.1 is shown. The proofs of Theorems 1.2 and 1.3 are given in Section 4.

2. Basic ingredients of Garside theory

In this section we will explain the notions and results that will be used throughout the rest of the paper. Namely, we will briefly describe the basic ingredients of the Garside structure of braid groups. In general, a Garside group is a group satisfying the structural properties defined in this section, and the main examples are braid groups and Artin–Tits groups of spherical type. For a short introduction to Garside theory, with a precise definition of a Garside group, see [6].

The braid group on n strands B_n can be defined by its well-known group presentation [3]:

$$B_n = \left\langle \sigma_1, \ldots, \sigma_{n-1} \;\middle|\; \begin{array}{l} \sigma_i\sigma_j = \sigma_j\sigma_i, \text{ if } |j-i| > 1 \\ \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j, \text{ if } |j-i| = 1 \end{array} \right\rangle. \tag{1}$$

If we consider the above as a monoid presentation, this defines the monoid B_n^+, called the monoid of *positive braids*. Garside [17] showed that B_n^+ embeds into B_n, so the elements of B_n^+ can be seen as the braids in B_n that can be written as a word which only contains positive powers of the generators. There is a special positive element, called *half-twist* or **Garside element**, defined by $\Delta = \sigma_1(\sigma_2\sigma_1)\cdots(\sigma_{n-1}\cdots\sigma_1)$. Artin [3] showed that the centre of B_n is the cyclic subgroup generated by Δ^2. In general, every Garside group G has a distinguished monoid G^+ of positive elements which embeds into G, and a special Garside element, also denoted by Δ, which has a central power Δ^e. Conjugation by Δ is an inner automorphism which preserves the set of positive elements; we denote this automorphism by τ.

In a Garside group G, for example $G = B_n$, one can define two partial orders, related to left and right divisibility, respectively. Namely, given $a, b \in G$ we say that $a \preccurlyeq b$ if $a^{-1}b \in G^+$, that is, if $ap = b$ for some positive element p. We then say that a is a **left-divisor**, or a **prefix** of b. Similarly, we say that $a \succcurlyeq b$ if $ab^{-1} \in G^+$, that is, if $a = pb$ for some positive element p. In this case we say that b is a **right-divisor**, or a **suffix** of a. In general, $a \preccurlyeq b$ does not imply $b \succcurlyeq a$ or vice versa. But notice that $G^+ = \{p \in G \,:\, 1 \preccurlyeq p\} = \{p \in G \,:\, p \succcurlyeq 1\}$.

Each of the above partial orders defines a lattice structure on G. This means that given two elements $a, b \in G$, there exist a unique greatest common divisor (gcd) $a \wedge_L b$ and a unique least common multiple (lcm) $a \vee_L b$ with respect to the left divisibility relation $\preccurlyeq$, and also a unique gcd $a \wedge_R b$ and a unique lcm $a \vee_R b$ with respect to the right divisibility relation $\succcurlyeq$.

In B_n, the generators $\sigma_1, \ldots, \sigma_{n-1}$ are called **atoms**. In general, in a Garside group, an atom is a non-trivial positive element that cannot be decomposed as a product of two non-trivial positive elements. The set of atoms is preserved by the inner automorphism τ. In the particular case of B_n and of Artin–Tits groups of spherical type in their Artin Garside structure, the Garside element Δ is the (left and right) least common multiple of all atoms. This is not true in general for other Garside groups, and this is one of the reasons why the proof of Theorem 1.1 above cannot be generalised to every Garside group.

Several normal forms for elements of braid groups or Garside groups have been defined. We will focus on the one defined independently by Adyan [1], Deligne [14], Elrifai–Morton [15] and Thurston [16], which is an improvement of the one used in the solution to the word problem in B_n given by Garside [17]. We say that an element is **simple** if it is a positive prefix of the Garside element Δ. It is well known that this is the case if and only if the element is a positive suffix of Δ. The set S of simple elements of a Garside group G is then given by $S = \{s \in G \ : \ 1 \preccurlyeq s \preccurlyeq \Delta\} = \{s \in G \ : \ \Delta \succcurlyeq s \succcurlyeq 1\}$. The set of simple elements is preserved by the inner automorphism τ.

Definition 2.1. Given two simple elements s, s', we say that the decomposition ss' is **left-weighted** if s is the maximal simple prefix of ss', that is, if $s = (ss') \wedge_L \Delta$. Similarly, we say that ss' is **right-weighted** if s' is the maximal simple suffix of ss', that is, if $s' = (ss') \wedge_R \Delta$.

For a simple element s we call $\partial(s) = s^{-1}\Delta$ the **right complement** of s. Note that as $1 \preccurlyeq s \preccurlyeq \Delta$ and $s\,\partial(s) = \Delta$, the element $\partial(s)$ is simple. Hence, this defines a map $\partial : S \to S$ on the set S of simple elements. As we have $\partial(\partial(s)) = \Delta^{-1}s\Delta = \tau(s)$ for any simple element s, the map ∂ is a bijection on S which satisfies $\partial^2 = \tau$. We similarly define the **left complement** of s as $\Delta s^{-1} = \Delta\partial(s)\Delta^{-1} = \tau^{-1}(\partial(s)) = \partial^{-1}(s)$.

The right (resp. left) complement of s is the maximal element with respect to $\preccurlyeq$ (resp. $\succcurlyeq$) with which s can be multiplied from the right (resp. left) such that the product remains simple. Observe that, given two simple elements s and s', the product ss' is left-weighted if and only if there is no prefix $t \preccurlyeq s'$ such that st is simple, or in other words, such that $t \preccurlyeq \partial(s)$. Hence ss' is left-weighted if and only if $\partial(s) \wedge_L s' = 1$. Similarly, ss' is right-weighted if and only if $s \wedge_R \partial^{-1}(s') = 1$.

Definition 2.2. Given an element x of a Garside group G, its **left normal form** is the decomposition $x = \Delta^p x_1 \cdots x_r$, satisfying the following conditions:

(1) $p \in \mathbb{Z}$ is the maximal integer such that $\Delta^{-p}x$ is positive.
(2) $x_i = (x_i \cdots x_r) \wedge_L \Delta \neq 1$ for $i = 1, \ldots, r$.

In other words, each x_i is a proper simple element (different from 1 and Δ), and it is the maximal (with respect to $\preccurlyeq$) simple prefix of $x_i \cdots x_r$. It is well known that left normal forms can be recognised 'locally'. This means that $\Delta^p x_1 \cdots x_r$ is in left normal form if and only if each x_i is a proper simple element and $x_i x_{i+1}$ is left-weighted for $i = 1, \ldots, r-1$. The left normal form of x exists and it is unique. The integers p and r as above are then uniquely determined by x, whence we can define the **infimum**, **supremum** and **canonical length** of x, respectively, by $\inf(x) = p$, $\sup(x) = p+r$ and $\ell(x) = r$. This terminology is explained by noticing that p and $p+r$ are, respectively, the biggest and the smallest integers such that $\Delta^p \preccurlyeq x \preccurlyeq \Delta^{p+r}$, which is usually written $x \in [\Delta^p, \Delta^{p+r}]$, or simply $x \in [p, p+r]$. The canonical length r is just the size of this interval, which corresponds to the number of non-Δ factors in the left normal form of x.

We note that one has the analogous definitions related to $\succcurlyeq$:

Definition 2.3. Given an element x of a Garside group G, its **right normal form** is the decomposition $x = y_1 \cdots y_r \Delta^p$, satisfying the following conditions:

(1) $p \in \mathbb{Z}$ is the maximal integer such that $x\Delta^{-p}$ is positive.
(2) $y_i = (y_1 \cdots y_i) \wedge_R \Delta \neq 1$ for $i = 1, \ldots, r$.

Right normal forms also can be recognised locally (by checking that $y_i y_{i+1}$ is right-weighted for every i), and the right normal form of x also exists and is unique. We remark that the integers p and r in this case are exactly the same as those occurring in the left normal form of x. This means that $\inf(x) = p$ and $\sup(x) = p + r$ are, respectively, the maximal and minimal integers such that $\Delta^{p+r} \succcurlyeq x \succcurlyeq \Delta^p$, whence $\inf(x)$, $\sup(x)$ and $\ell(x)$ can equally be defined using right normal forms instead of left normal forms.

Let now G be a Garside group. Recall that we defined the initial factor of a braid in the introduction. Since we are using two distinct structures in G, we will define left and right versions of initial and final factors of $x \in G$ as follows. Given $x = \Delta^p x_1 \cdots x_r$ in left normal form with $r > 0$, we define its **left initial factor** as $\iota_L(x) = \tau^{-p}(x_1)$, and its **left final factor** by $\varphi_L(x) = x_r$. If $r = 0$, we define $\iota_L(x) = 1$ and $\varphi_L(x) = \Delta$. In the same way, given $x = y_1 \cdots y_r \Delta^p$ in right normal form with $r > 0$, we define its **right initial factor** by $\iota_R(x) = \tau^p(y_r)$, and its **right final factor** by $\varphi_R(x) = y_1$. If $r = 0$, we define $\iota_R(x) = 1$ and $\varphi_R(x) = \Delta$.

There are special maps from G to itself that consist of conjugating each element by its initial or final factors. These operations, called (left or right) *cycling* and *decycling*, are key ingredients in most of the known solutions to the conjugacy problem in braid groups and Garside groups in general. The precise definition is as follows; we write the conjugate of x by a conjugating element c as $x^c = c^{-1}xc$.

Definition 2.4. The following maps, from G to itself, are defined for each $x \in G$ as follows:

(1) **Left cycling:** $\mathbf{c}_L(x) = \iota_L(x)^{-1} \cdot x \cdot \iota_L(x) = x^{\iota_L(x)}$
(2) **Left decycling:** $\mathbf{d}_L(x) = \varphi_L(x) \cdot x \cdot \varphi_L(x)^{-1} = x^{\varphi_L(x)^{-1}}$
(3) **Right cycling:** $\mathbf{c}_R(x) = \iota_R(x) \cdot x \cdot \iota_R(x)^{-1} = x^{\iota_R(x)^{-1}}$
(4) **Right decycling:** $\mathbf{d}_R(x) = \varphi_R(x)^{-1} \cdot x \cdot \varphi_R(x) = x^{\varphi_R(x)}$.

In other words, if $x = \Delta^p x_1 \cdots x_r$ is in left normal form, then

$$\mathbf{c}_L(x) = \Delta^p x_2 \cdots x_r \tau^{-p}(x_1), \qquad \mathbf{d}_L(x) = x_r \Delta^p x_1 \cdots x_{r-1},$$

and if $x = y_1 \cdots y_r \Delta^p$ is in right normal form, then

$$\mathbf{c}_R(x) = \tau^p(y_r) y_1 \cdots y_{r-1} \Delta^p, \qquad \mathbf{d}_R(x) = y_2 \cdots y_r \Delta^p y_1.$$

We note that there is an involution of the braid group, $\mathrm{rev} : B_n \to B_n$, which sends every braid $x = \sigma_{i_1}^{e_1} \cdots \sigma_{i_m}^{e_m}$ to its **reverse** $\mathrm{rev}(x) = \overleftarrow{x} = \sigma_{i_m}^{e_m} \cdots \sigma_{i_1}^{e_1}$, that is, the same word read backwards. Observe that the map rev is well defined, as the relations of B_n are invariant under rev. The map rev is an anti-isomorphism. For a general Garside group, one can similarly define an anti-isomorphism $\mathrm{rev} : G \to \overleftarrow{G}$ whose image $\overleftarrow{G}$ can be seen to be also a Garside group. (If $G = B_n$, we have $\overleftarrow{G} = G$, but this need not be the case in general.) One can easily check that the left normal form of x (in G) is mapped by rev to the right normal form of $\overleftarrow{x}$ (in $\overleftarrow{G}$), and vice versa. Also $\overleftarrow{\iota_R(x)} = \iota_L(\overleftarrow{x})$, $\overleftarrow{\varphi_R(x)} = \varphi_L(\overleftarrow{x})$, and hence $\overleftarrow{\mathbf{c}_R(x)} = \mathbf{c}_L(\overleftarrow{x})$ and $\overleftarrow{\mathbf{d}_R(x)} = \mathbf{d}_L(\overleftarrow{x})$. This means that applying $\mathbf{c}_R$ and $\mathbf{d}_R$ to an element x corresponds to applying the usual (left) cycling and decycling operations, $\mathbf{c}_L$ and $\mathbf{d}_L$, to its reverse $\overleftarrow{x}$. This implies that all results which are usually shown using left normal forms, $\mathbf{c}_L$ and $\mathbf{d}_L$, also hold using right normal forms, $\mathbf{c}_R$ and $\mathbf{d}_R$, by symmetry.

Cyclings and decyclings have been used to define suitable finite subsets of conjugacy classes of elements, which allow us to solve the conjugacy decision problem and the conjugacy search problem. For instance, the **super summit set** [15] of an element x, denoted by $\mathrm{SSS}(x)$, is defined as follows. If we denote the conjugacy class of x by $C(x)$, then

$$\mathrm{SSS}(x) = \{y \in C(x) : \ell(y) \text{ is minimal among all elements of } C(x)\}.$$

Notice that this set does not depend on whether left or right normal forms are used to define $\ell(y)$. A subset of $\mathrm{SSS}(x)$ is the *ultra summit set* of x [18]. In this case, since $\mathrm{USS}(x)$ is defined using cyclings, one needs to distinguish between the **left ultra summit set** of x,

$$\mathrm{USS}_L(x) = \{y \in \mathrm{SSS}(x) : \exists\, t \geq 1, \mathbf{c}_L^t(y) = y\},$$

and the **right ultra summit set** of x,

$$\mathrm{USS}_R(x) = \{y \in \mathrm{SSS}(x) : \exists\, t \geq 1, \mathbf{c}_R^t(y) = y\}.$$

Both $\mathrm{SSS}(x)$, $\mathrm{USS}_L(x)$ and $\mathrm{USS}_R(x)$ are, by definition, invariants of the conjugacy class of x and they are non-empty subsets of $C(x)$. Hence one can determine whether two elements x and y are conjugate by computing, say, $\mathrm{USS}_L(x)$ and $\mathrm{USS}_L(y)$ and checking whether these sets are equal. Actually, it suffices to compute $\mathrm{USS}_L(x)$ and one element $y' \in \mathrm{USS}_L(y)$ and to check whether $y' \in \mathrm{USS}_L(x)$. In [15] it is shown how to compute $\mathrm{SSS}(x)$, and [18] gives an algorithm to compute $\mathrm{USS}_L(x)$ (which can also be used to compute $\mathrm{USS}_R(x)$). More precisely, the algorithm computes a directed graph whose set of vertices is $\mathrm{USS}_L(x)$. We will define such a graph as follows.

Definition 2.5. Given $x \in G$, we define the **left ultra summit graph** of x, denoted by $\mathrm{USG}_L(x)$, as the directed graph whose set of vertices is $\mathrm{USS}_L(x)$ and whose arrows are labelled by simple elements, in such a way that there is an arrow labelled by s, starting at u and ending at v, if $s^{-1}us = v$.

In the same way, we define the **right ultra summit graph** of x, denoted by $\mathrm{USG}_R(x)$, as the directed graph whose set of vertices is $\mathrm{USS}_R(x)$ and whose arrows are labelled by simple elements, in such a way that there is an arrow labelled by s, starting at u and ending at v, if $sus^{-1} = v$.

We remark that the graph computed in [18] is not precisely $\mathrm{USG}_L(x)$, but one with fewer arrows:

Definition 2.6. Given $x \in G$, we define the graph $\mathrm{minUSG}_L(x)$ to be the subgraph of $\mathrm{USG}_L(x)$ with the same set of vertices, but only with **minimal** arrows. An arrow labelled by s and starting at u is said to be minimal if it cannot be decomposed as a product of arrows, that is, if there is no directed path in $\mathrm{USG}_L(x)$ starting at u, with labels $s_1, \ldots, s_k$, such that $s = s_1 \cdots s_k$.

In the same way, we define the graph $\mathrm{minUSG}_R(x)$ to be the subgraph of $\mathrm{USG}_R(x)$ with the same set of vertices, but only with minimal arrows.

It is known that all the above graphs are connected. The arrows in these graphs indicate how to connect, by conjugations, x to any element in $\mathrm{USS}_L(x)$ and y to any element in $\mathrm{USS}_L(y)$. Hence, the above procedure also solves the conjugacy search problem in any Garside group G (and hence in particular the conjugacy search problem in the braid group B_n), that is, it finds a conjugating element from x to y provided such an element exists.

In [6] is the description of a project to find a polynomial solution to the conjugacy search problem in braid groups. One of the crucial open problems in this project concerns *rigid* braids. We can define rigid elements for every Garside group G. As above, since we are using two different structures on G, we will define left rigid and right rigid elements. We say that an element x whose left normal form is $x = \Delta^p u_1 \cdots u_r$ with $r > 0$ is **left rigid**, if $\Delta^p u_1 \cdots u_r \iota_L(x)$ is in left normal form as written. In the same way, we will say that x is **right rigid**, if its right normal form is $x = v_1 \cdots v_r \Delta^p$ with $r > 0$ and $\iota_R(x) v_1 \cdots v_r \Delta^p$ is in right normal form as written, or equivalently, if $\overleftarrow{x}$ is left rigid. Rigid elements have the best possible behaviour with respect to cyclings and decyclings, since in this case iterated cyclings or decyclings just correspond to cyclic permutations of the factors. For nonrigid elements this is not the case, since one has to compute the left normal form of $\mathbf{c}_L(x)$ in order to be able to apply $\mathbf{c}_L$ again, which modifies some of the original factors of x.

There are some interesting results concerning rigid elements in general and rigid braids in particular:

Theorem 2.7 (*[6]*). *If G is a Garside group and $x \in G$ is left (resp. right) rigid then $x \in \mathrm{USS}_L(x)$ (resp. $x \in \mathrm{USS}_R(x)$). Moreover, if $\ell(x) > 1$ then $\mathrm{USS}_L(x)$ (resp. $\mathrm{USS}_R(x)$) is precisely the set of left (resp. right) rigid conjugates of x.*

Theorem 2.8 (*[6]*). *If $x \in B_n$ is a pseudo-Anosov braid, and $x \in \mathrm{USS}_L(x)$ (resp. $x \in \mathrm{USS}_R(x)$), then x^m is left (resp. right) rigid for some $m < (\frac{n(n-1)}{2})^3$.*

Since pseudo-Anosov braids seem to be generic in B_n, and the conjugacy search problem for pseudo-Anosov braids x and y can be solved just by solving it for x^m and y^m for any $m \neq 0$ [19], the rigid case turns out to be probably the most important case for solving the conjugacy search problem in B_n.

As was noticed in [18], if the canonical length of a random braid x is big enough, then $\mathrm{USS}_L(x)$ consists of exactly $2\ell(x)$ elements in 100% of the tested cases, meaning that the probability of getting a larger $\mathrm{USS}_L(x)$ seems to tend to zero very rapidly as $\ell(x)$ grows. Moreover, in these 'generic' cases the braids in $\mathrm{USS}_L(x)$ are pseudo-Anosov and left rigid. We remark that the algorithm in [18] is a deterministic solution to the conjugacy problem and the conjugacy

search problem that seems to be 'generically' polynomial, although there is no written proof, to our knowledge, that either pseudo-Anosov braids or braids conjugate to a rigid element are generic in B_n.

There are, however, instances of left rigid braids whose ultra summit set is much larger than expected. For instance, as is noticed in [6], the braid in B_{12}

$$E = (\sigma_2\sigma_1\sigma_7\sigma_6\sigma_5\sigma_4\sigma_3\sigma_8\sigma_7\sigma_{11}\sigma_{10}) \cdot (\sigma_1\sigma_2\sigma_3\sigma_2\sigma_1\sigma_4\sigma_3\sigma_{10}) \cdot (\sigma_1\sigma_3\sigma_4\sigma_{10}) \cdot (\sigma_1\sigma_{10}) \cdot (\sigma_1\sigma_{10}\sigma_9\sigma_8\sigma_7\sigma_{11}) \cdot (\sigma_1\sigma_2\sigma_7\sigma_{11})$$

is a pseudo-Anosov, left rigid braid with canonical length $\ell(E) = 6$, and we find $\#(\mathrm{USS}_L(E)) = 264 = 44 \cdot 6$, instead of the expected value of $12 = 2 \cdot 6$. Also, the braid in B_{12}

$$F = (\sigma_3\sigma_2\sigma_1\sigma_4\sigma_6\sigma_8\sigma_7\sigma_6\sigma_9\sigma_{10}\sigma_{11}\sigma_{10}) \cdot (\sigma_1\sigma_2\sigma_4\sigma_3\sigma_2\sigma_1\sigma_5\sigma_7\sigma_{10}\sigma_{11}\sigma_{10}) \cdot (\sigma_3\sigma_5\sigma_7\sigma_{10}\sigma_{11}\sigma_{10}) \cdot (\sigma_3\sigma_5\sigma_7\sigma_6\sigma_8\sigma_{10}\sigma_{11})$$

is pseudo-Anosov and left rigid, with canonical length $\ell(F) = 4$ and we find $\#(\mathrm{USS}_L(F)) = 232 = 58 \cdot 4$, instead of the expected value of $8 = 2 \cdot 4$. The reason why these special examples of rigid braids exist, and how one can construct them, is still a mystery. Solving this problem would be an important step towards finding secure keys for cryptographic protocols with braid groups.

Now recall that we have two distinct structures on B_n. It could be possible, a priori, that $\mathrm{USS}_R(E)$ or $\mathrm{USS}_R(F)$ are much smaller than $\mathrm{USS}_L(E)$ or $\mathrm{USS}_L(F)$, respectively. However, Theorem 1.3 tells us that this is not the case, since $\#(\mathrm{USS}_R(x)) = \#(\mathrm{USS}_L(x))$ for every rigid braid x of canonical length greater than 1.

3. Cycling is surjective

In this section we will show Theorem 1.1, that is, we will show that $\mathbf{c}_L$ (and thus $\mathbf{c}_R$) is a surjective map.

First recall the definition of the right complement $\partial(s)$ of a simple element s from Definition 2.1. A product ss' of two simple elements s and s' is left-weighted if and only if $\partial(s) \wedge_L s' = 1$.

It was shown by Maffre [24] that the pre-image of an element x of a Garside group under $\mathbf{c}_L$ can be computed fast, provided that x is in the image of $\mathbf{c}_L$. More precisely, he shows the following:

Theorem 3.1 (*[24, Proposition 7.2.10]*). *Let G be a Garside group and let x be an element of G with* $\inf(x) = p$. *Then*

(1) $\mathbf{c}_L(y) = x$ *for some element* $y \in G$ *with* $\inf(y) = p - 1$, *if and only if* $\mathbf{c}_L(\tau^{-1}(a^{-1}xa)) = x$ *for some atom* a.
(2) $\mathbf{c}_L(y) = x$ *for some element* $y \in G$ *with* $\inf(y) = p$, *if and only if* $\mathbf{c}_L(\mathbf{c}_R(x)) = x$.

It is clear by definition that cycling cannot decrease the infimum of an element, and it is well known that it may increase it by at most one. Hence, the above result shows how to compute a pre-image of an element under left cycling, provided such a pre-image exists. Notice in particular that in order to find a pre-image, one just needs to check the candidates given by Theorem 3.1, that is, at most $t + 1$ elements, where t is the number of atoms in G. If we denote the complexity of computing a left normal form by L, then the complexity of computing a pre-image of x under left cycling is $O(tL)$, since conjugating by an atom, applying τ^{-1}, computing a right normal form or applying a left or right cycling, are all computations that have at most the same complexity as computing a left normal form. For instance, in the braid group B_n with the Artin structure, one has $t = n - 1$ and $L = r^2 n \log n$, where r is the canonical length of x. Hence, computing a pre-image of $x \in B_n$ under left cycling, provided a pre-image exists, has complexity $O(r^2 n^2 \log n)$.

Theorem 1.1 states that for some Garside groups, which we call atom-friendly, at least one of the two cases in Theorem 3.1 always occurs. In order to show this, we will not focus on the infimum of a possible pre-image of x, but on the behaviour of the atoms with respect to the left normal form of x. The first case, given by the following result, holds for every Garside group G, not necessarily atom-friendly. It is implicitly contained in Section 7.2 of [24], although we will give an alternative proof to make this paper self-contained.

Proposition 3.2 (*[24]*). *Let G be a Garside group, let x be an element of G, and let $x = \Delta^p x_1 \cdots x_r$ be written in left normal form. If there is an atom a such that $\tau^p(a) \not\preccurlyeq x_1 \cdots x_r a$, then $\mathbf{c}_L(\tau^{-1}(a^{-1}xa)) = x$.*

Proof. Define $z = a^{-1}xa = \partial(a)\Delta^{p-1}x_1 \cdots x_r a = \Delta^{p-1}\partial^{2p-1}(a)x_1 \cdots x_r a$. Notice that $\partial(\partial^{2p-1}(a)) = \partial^{2p}(a) = \tau^p(a) \not\preccurlyeq x_1 \cdots x_r a$. As τ transforms atoms into atoms, $\tau^p(a)$ is an atom. This means that $\tau^p(a) \not\preccurlyeq x_1 \cdots x_r a$ is equivalent to $\tau^p(a) \wedge_L x_1 \cdots x_r a = 1$, since an atom has no non-trivial prefixes.

Notice that $\Delta \not\preccurlyeq x_1 \cdots x_r a$, otherwise $\tau^p(a) \preccurlyeq \Delta \preccurlyeq x_1 \cdots x_r a$. Hence, the left normal form of $x_1 \cdots x_r a$ is of the form $z_2 \cdots z_k$ and, moreover, we have $\partial(\partial^{2p-1}(a)) \wedge_L z_2 = \tau^p(a) \wedge_L z_2 = \tau^p(a) \wedge_L x_1 \cdots x_r a \wedge_L \Delta = 1$, that is, $\partial^{2p-1}(a)z_2$ is left-weighted. This implies that $\partial^{2p-1}(a)z_2 \cdots z_k$ is the left normal form of $\partial^{2p-1}(a)x_1 \cdots x_r a$. Hence, $\iota_L(z) = \tau^{-p+1}(\partial^{2p-1}(a)) = \partial^{-2p+2}(\partial^{2p-1}(a)) = \partial(a)$.

If we apply left-cycling to z, we then obtain

$$\mathbf{c}_L(z) = z^{\partial(a)} = \Delta^{p-1}x_1 \cdots x_r a\partial(a) = \Delta^{p-1}x_1 \cdots x_r \Delta = \tau(x).$$

It is well known (and can be derived from the definitions and from the fact that τ is a bijection of S) that τ sends left (resp. right) normal forms to left (resp. right) normal forms. Hence τ commutes with $\mathbf{c}_L$ (resp. $\mathbf{c}_R$). Therefore $\mathbf{c}_L(\tau^{-1}(z)) = \tau^{-1}(\mathbf{c}_L(z)) = \tau^{-1}(\tau(x)) = x$, as we wanted to show. □

We will now see that, if the hypothesis of Proposition 3.2 is not satisfied, the second case in Theorem 3.1 occurs, that is, a pre-image of x under $\mathbf{c}_L$ is just given by $\mathbf{c}_R(x)$. However, this time our proof does not work for every Garside group, but we need some special property to be satisfied. Given a Garside group G, we denote the set of atoms by $\mathcal{A}$. Given a simple element $s \in G$, we define the **starting set** of s as $\mathcal{S}(s) = \{a \in \mathcal{A} \,:\, a \preccurlyeq s\}$.

Definition 3.3. Given a Garside group G, we say that G is **atom-friendly** (on the left) if

(1) $\mathrm{lcm}_L(\mathcal{A}) = \Delta$.
(2) $\mathcal{S}(\mathrm{lcm}_L(\mathcal{B})) = \mathcal{B}$ for every $\mathcal{B} \subset \mathcal{A}$.

Example 3.4. We give a simple example of a Garside group which is not atom-friendly. It is well known [9] that braid groups, apart from the Garside structure induced by presentation (1) which was discussed in Section 2, admit another Garside structure, the so-called *dual Garside structure*. The latter is induced by the presentation with the generators $\{a_{t,s} \text{ for } n \geq t > s \geq 1\}$ subject to the relations

$$\left\{a_{t,s}a_{r,q} = a_{r,q}a_{t,s},\ \text{if } (t-r)(t-q)(s-r)(s-q) > 0, a_{t,s}a_{s,r} = a_{t,r}a_{t,s} = a_{s,r}a_{t,r},\ \text{if } t > s > r\right\}.$$

Its atoms are precisely the generators $a_{t,s}$ and its Garside element is given by $\delta = a_{n,n-1}a_{n-1,n-2} \cdots a_{2,1}$. In terms of presentation (1), the generators $a_{t,s}$ can be expressed as $a_{t,s} = (\sigma_{t-1} \cdots \sigma_{s+1})\sigma_s(\sigma_{s+1}^{-1} \cdots \sigma_{t-1}^{-1})$.

It is easy to see that even for $n = 3$ this Garside structure is not atom-friendly: For $\mathcal{B} = \{a_{3,1}, a_{3,2}\}$ one has $\mathrm{lcm}_L(\mathcal{B}) = \delta = a_{3,1}a_{3,2} = a_{3,2}a_{2,1} = a_{2,1}a_{3,1}$, whence $\mathcal{S}(\mathrm{lcm}_L(\mathcal{B})) = \mathcal{A} \neq \mathcal{B}$.

Remark 3.5. We remark that the terminology *atom-friendly* is new. To our knowledge, no common name has been given to those Garside groups satisfying the above two conditions. It is nevertheless well known [25] that the Artin Garside structures of braid groups, and more generally of Artin–Tits groups of spherical type, are atom-friendly (on the left and on the right). Hence the following result holds in all Artin–Tits groups of spherical type endowed with the Artin Garside structure.

Note, however, that each Artin–Tits group of spherical type also admits a different Garside structure, the *dual Garside structure* [5]. The latter *is not atom-friendly* in general, as we saw in Example 3.4 for the case of the braid group on three strands.

Proposition 3.6. *Let G be a Garside group which is atom-friendly (on the left). Let $x = \Delta^p x_1 \cdots x_r \in G$ be written in left normal form. If for every atom a one has $\tau^p(a) \preccurlyeq x_1 \cdots x_r a$, then $\mathbf{c}_L(\mathbf{c}_R(x)) = x$.*

Proof. Let us define $\mathcal{D}$ to be the set of atoms a such that $\tau^p(a) \not\preccurlyeq x_1$. That is $\mathcal{D} = \mathcal{A} \setminus \mathcal{S}(\tau^{-p}(x_1)) = \mathcal{A} \setminus \mathcal{S}(\iota_L(x))$. Moreover, we define the simple element $D = \mathrm{lcm}_L(\mathcal{D})$. Let us show that $\Delta \preccurlyeq x_1 \cdots x_r D$. Indeed, for every atom $a \notin \mathcal{D}$ one has $\tau^p(a) \preccurlyeq x_1 \preccurlyeq x_1 \cdots x_r D$, and for every atom $a \in \mathcal{D}$ one has $a \preccurlyeq D$, so using the hypothesis it follows that $\tau^p(a) \preccurlyeq x_1 \cdots x_r a \preccurlyeq x_1 \cdots x_r D$. Therefore $\tau^p(a) \preccurlyeq x_1 \cdots x_r D$ for every atom a. Since τ^p induces a permutation on the set of atoms, this means that $a \preccurlyeq x_1 \cdots x_r D$ for every atom a. But since G is atom-friendly, $\Delta = \mathrm{lcm}(\mathcal{A})$, hence we finally obtain that $\Delta \preccurlyeq x_1 \cdots x_r D$.

Now let $z_1 \cdots z_r$ be the right normal form of $x_1 \cdots x_r$. We just showed that $\Delta \preccurlyeq z_1 \cdots z_r D$, but this is equivalent to $z_1 \cdots z_r D \succcurlyeq \Delta$. Since $z_1 \cdots z_r$ is in right normal form, this implies that $z_r D \succcurlyeq \Delta$, which is equivalent to $\Delta \preccurlyeq z_r D$ or, in other words, $\partial(z_r) \preccurlyeq D$.

Now we use again that G is atom-friendly, so $\mathcal{S}(D) = \mathcal{D}$. As $\mathcal{D} = \mathcal{A} \setminus \mathcal{S}(\iota_L(x))$, one has that $\mathcal{S}(D) \cap \mathcal{S}(\iota_L(x)) = \emptyset$. Hence, $D \wedge_L \tau^{-p}(x_1) = D \wedge_L \iota_L(x) = 1$, which is equivalent to $\tau^p(D) \wedge_L x_1 = 1$.

Finally, consider $y = \mathbf{c}_R(x) = x^{z_r^{-1}} = \Delta^p \tau^p(z_r) z_1 \cdots z_{r-1}$. We will show that $\mathbf{c}_L(y) = x$. Recall that $\partial(z_r) \preccurlyeq D$, hence $\partial(\tau^p(z_r)) \preccurlyeq \tau^p(D)$. On the other hand, $z_1 \cdots z_{r-1} \preccurlyeq z_1 \cdots z_r = x_1 \cdots x_r$. Hence, if we define $\alpha = \Delta \wedge_L z_1 \cdots z_{r-1}$, we have $\alpha \preccurlyeq \Delta \wedge_L z_1 \cdots z_r = \Delta \wedge_L x_1 \cdots x_r = x_1$. But since $\tau^p(D) \wedge_L x_1 = 1$, and we are considering left divisors $\partial(\tau^p(z_r)) \preccurlyeq \tau^p(D)$ and $\alpha \preccurlyeq x_1$, it follows that $\partial(\tau^p(z_r)) \wedge_L \alpha = 1$. In other words, $\tau^p(z_r)\alpha$ is left-weighted as written, whence $\tau^p(z_r)$ is the first factor in the left normal form of $\tau^p(z_r) z_1 \cdots z_{r-1}$. Therefore, $\mathbf{c}_L(y) = y^{z_r} = x$, as we wanted to show. □

We have thus shown Theorem 1.1, since Propositions 3.2 and 3.6 run over all possibilities.

4. Rigid ultra summit sets

4.1. Left rigid and right rigid elements

In this section we will show Theorem 1.2. Let $x \in B_n$, and recall the definitions of $\mathrm{USS}_L(x)$ and $\mathrm{USS}_R(x)$ given in Section 2. Since the statement of Theorem 1.2 refers to the conjugacy class of x, and not to x itself, we can assume that $x \in \mathrm{SSS}(x)$, that is, x has maximal infimum and minimal supremum in its conjugacy class. We will see how one can determine if x is conjugate to a rigid braid by looking at its powers. First we will see that if x is conjugate to a rigid element, then the infimum and supremum of its powers behave as one should expect.

Definition 4.1. An element x of a Garside group is called **periodically geodesic** if $\inf(x^m) = m \inf(x)$ and $\sup(x^m) = m \sup(x)$ for every $m \geq 1$.

The two following Lemmas are known. However, as their proofs are simple, we include them for convenience.

Lemma 4.2 (*[22]*). *Let x be an element of a Garside group. If $x \in \mathrm{SSS}(x)$ and x is conjugate to a (left or right) rigid element, then x is periodically geodesic.*

Proof. Let $p = \inf(x)$, $q = \sup(x)$ and let y be a left rigid conjugate of x. Then y is periodically geodesic and $y^m \in \mathrm{USS}(x^m) \subset \mathrm{SSS}(x^m)$ for any $m \in \mathbb{Z}$. In particular, $\inf(y^m) = m \inf(y) = mp$ and $\sup(y^m) = m \sup(y) = mq$. As super summit elements have maximal infimum and minimal supremum in their conjugacy class, we obtain $mp = m \inf(x) \leq \inf(x^m) \leq \inf(y^m) = mp$ and $mq = m \sup(x) \geq \sup(x^m) \geq \sup(y^m) = mq$, which shows that x is periodically geodesic.

The right rigid case is analogous. □

The above result is not the only one relating periodically geodesic and rigid elements.

Lemma 4.3 (*[20]*). *Let x be an element in a Garside group G. If x is periodically geodesic and x^m is left (resp. right) rigid for some $m \geq 1$, then x is left (resp. right) rigid.*

Proof. We assume that x^m is left rigid; the right rigid case is analogous. Let $\Delta^p x_1 \cdots x_r$ be the left normal form of x. Since x is periodically geodesic, the left normal form of x^m is $\Delta^{mp} z_1 \cdots z_{rm}$, where

$$z_1 \cdots z_{rm} = \tau^{(m-1)p}(x_1 \cdots x_r)\tau^{(m-2)p}(x_1 \cdots x_r) \cdots \tau^p(x_1 \cdots x_r)(x_1 \cdots x_r).$$

This means that $\tau^{(m-1)p}(x_1) \preccurlyeq z_1 \cdots z_{rm}$, which implies that $\tau^{(m-1)p}(x_1) \preccurlyeq z_1$, as $z_1 \cdots z_{rm}$ is in left normal form. Then, $\iota_L(x) = \tau^{-p}(x_1) \preccurlyeq \tau^{-mp}(z_1) = \iota_L(x^m)$.

In the same way, since the last simple factor in the above decomposition of $z_1 \cdots z_{rm}$ is x_r, and the number of factors is precisely rm, it follows that $x_r \succcurlyeq z_{rm}$. In other words, $\varphi_L(x) \succcurlyeq \varphi_L(x^m)$.

Finally, recall that x^m is left rigid, which means that $\varphi_L(x^m)\iota_L(x^m)$ is left-weighted as written, that is, we have $\partial(\varphi_L(x^m)) \wedge_L \iota_L(x^m) = 1$. Since the condition $\varphi_L(x) \succcurlyeq \varphi_L(x^m)$ is equivalent to $\partial(\varphi_L(x)) \preccurlyeq \partial(\varphi_L(x^m))$, we obtain that $\partial(\varphi_L(x)) \wedge_L \iota_L(x) \preccurlyeq \partial(\varphi_L(x^m)) \wedge_L \iota_L(x^m) = 1$. That is, $\varphi_L(x)\iota_L(x)$ is left-weighted as written, whence x is left rigid. □

Corollary 4.4. *Let G be a Garside group and let $x \in G$ such that $x \in \mathrm{SSS}(x)$. If x has a left rigid power and x is conjugate to a right rigid element, then x is left rigid. Also, if x has a right rigid power and x is conjugate to a left rigid element, then x is right rigid.*

Proof. This is a direct consequence of Lemmas 4.2 and 4.3. □

After this result, in order to show that every left rigid element is conjugate to a right rigid element, and vice versa, we must show that every left rigid element has a conjugate which has a right rigid power. In braid groups, this holds for pseudo-Anosov braids, since one has the following result.

Theorem 4.5 *([6, Theorem 3.23]). Let $x \in B_n$ be a pseudo-Anosov braid. If $x \in \mathrm{USS}_L(x)$ and $\ell(x) > 1$, then x has a left rigid power. In the same way, if $x \in \mathrm{USS}_R(x)$ and $\ell(x) > 1$, then x has a right rigid power.*

Corollary 4.6. *If $x \in B_n$ is a left (resp. right) rigid, pseudo-Anosov braid, and $\ell(x) > 1$, then x is conjugate to a right (resp. left) rigid braid.*

Proof. Suppose that x is left rigid, and consider $y \in \mathrm{USS}_R(x)$. By Theorem 4.5, the braid y has a right rigid power, hence y itself must be right rigid by Corollary 4.4. If x is right rigid, the proof follows the same reasoning. □

But there are two more kinds of braids, namely periodic and reducible ones. Does the above result hold for these ones? The answer is positive, as we shall see. We recall that a braid $x \in B_n$ is called **periodic** if $x^m = \Delta^t$ for some non-zero integers m and t. The above result holds trivially for periodic braids, due to the following lemma.

Lemma 4.7. *A left or right rigid braid can never be periodic.*

Proof. By definition, if $x \in B_n$ is (left or right) rigid then $\ell(x) > 0$. Also, by Lemma 4.2, x is periodically geodesic. Hence $\ell(x^m) = |m|\ell(x) > 0$ for every non-zero integer m. Thus, no power of x can be a power of Δ, since $\ell(\Delta^t) = 0$ for every t. □

It just remains to show the case of reducible braids. A braid $x \in B_n$ is said to be **reducible** if, regarding x as a homeomorphism of the n-times punctured disc, it preserves a family of disjoint, closed, essential curves, up to isotopy [10]. This can be expressed in other terms: A **non-trivial coherent tape structure** [4] for a braid $x \in B_n$ is a proper composition $\mathcal{T}$ of n (that is, $\mathcal{T} = (k_1, \ldots, k_m)$ where $k_1 + \cdots + k_m = n$, $1 < m < n$ and $k_i \geq 1$ for all i) such that x can be obtained from a braid $x_{\mathcal{T}} \in B_m$ by replacing, for each $i = 1, \ldots, m$, the ith strand of $x_{\mathcal{T}}$ by a braid $x_{[i]} \in B_{k_i}$. One can think that the ith strand of $x_{\mathcal{T}}$ becomes a tube, and that $x_{[i]}$ lies inside that tube. One further requirement is that the m-tuple $\mathcal{T} = (k_1, \ldots, k_m)$ is coherent with the permutation induced by $x_{\mathcal{T}}$, that is, if the ith strand of $x_{\mathcal{T}}$ ends at position j, then $k_i = k_j$. The braid $x_{\mathcal{T}}$ is called the **tubular** or **external** braid of this decomposition of x, while each $x_{[i]}$ is called the ith **internal** braid. A braid is then reducible if and only if one of its conjugates admits a non-trivial coherent tape structure.

We can now extend the result of Corollary 4.6 to all braids, that is, we can show the following result, which is equivalent to Theorem 1.2.

Theorem 4.8. *If $x \in B_n$ is a left (resp. right) rigid braid, and $\ell(x) > 1$, then x is conjugate to a right (resp. left) rigid braid.*

Proof. Suppose that x is left rigid; the proof for the other direction is analogous. We will show the result by induction on n. If $n = 1$, then x is trivial and there is nothing to show. If $n = 2$, then x is either trivial or periodic and hence cannot be rigid by Lemma 4.7. So suppose that $n > 2$ and that the result holds for braids with less than n strands.

If x is pseudo-Anosov, the result is given by Corollary 4.6. On the other hand, x cannot be periodic by Lemma 4.7. We hence can assume that x is reducible.

In [4] it was shown that if a braid α admits a non-trivial coherent tape structure, so do $\mathbf{c}_L(\alpha)$ and $\mathbf{d}_L(\alpha)$. This implies that for every reducible braid, there is some element in its left ultra summit set that admits a non-trivial coherent tape structure. Since we are assuming that x is left rigid and $\ell(x) > 1$, Theorem 2.7 yields that $\mathrm{USS}_L(x)$ is the set of left rigid conjugates of x, whence there is a conjugate of x which is left rigid and admits a non-trivial coherent tape structure. We can thus assume that x itself admits a non-trivial coherent tape structure $\mathcal{T} = (k_1, \ldots, k_m)$.

Now consider the external and internal braids [4] of x with respect to $\mathcal{T}$; let $x_{\mathcal{T}} \in B_m$ be the external braid and let $x_{[i]} \in B_{k_i}$ for $i = 1, \ldots, m$ (where $k_1 + \cdots + k_m = n$) be the internal braids. Observe that $\mathcal{T}$ is a non-trivial coherent tape structure for every power x^j of x and that the external braid of x^j with respect to $\mathcal{T}$ is $(x_{\mathcal{T}})^j$.

Let $y = \mathbf{c}_R^K(x) \in \mathrm{USS}_R(x)$, obtained from x by a finite number of applications of $\mathbf{c}_R$. By Corollary 4.4, we just need to show that y has a right rigid power. In order to simplify the notation, we will replace x by a power x^j such that the permutation induced by $(x_{\mathcal{T}})^j$ is trivial (that is, $(x_{\mathcal{T}})^j$ is a pure braid). Notice that x^j is also left rigid and if we show that y^j has a right rigid power, this will also be true for y. We can hence assume that $x_{\mathcal{T}}$ is a pure braid.

By the arguments in [4] applied to right normal forms, $y = \mathbf{c}_R^K(x)$ admits a non-trivial coherent tape structure $\mathcal{T}'$, such that the internal components of y with respect to $\mathcal{T}'$ canonically correspond to those of x with respect to $\mathcal{T}$, with the correspondence given by the action of the element conjugating x to y. We label the internal braids of y by $y_{[i]} \in B_{k_i}$ in accordance with this correspondence and denote the external braid of y by $y_{\mathcal{T}'} \in B_m$. It can, moreover, be seen from [4] that $y_{\mathcal{T}'}$ is a conjugate of $x_{\mathcal{T}}$, whence $y_{\mathcal{T}'}$ is also a pure braid, as the pure braid group is normal in B_m.

Let $p = \inf(x)$ and $q = \sup(x) > p + 1$. Let $\varphi_L(x)_{\mathcal{T}}$ be the external component and $\varphi_L(x)_{[i]}$ the ith internal component of $\varphi_L(x)$ with respect to the decomposition of x by $\mathcal{T}$. In the same way, define $\iota_L(x)_{\mathcal{T}}$, $\iota_L(x)_{[i]}$, $\varphi_R(x)_{\mathcal{T}}$, $\varphi_R(x)_{[i]}$, $\iota_R(x)_{\mathcal{T}}$ and $\iota_R(x)_{[i]}$. Analogously, using $\mathcal{T}'$, define $\varphi_R(y)_{\mathcal{T}'}$, $\varphi_R(y)_{[i]}$, $\iota_R(y)_{\mathcal{T}'}$ and $\iota_R(y)_{[i]}$. As x is left rigid, we have $\partial(\varphi_L(x)) \wedge_L \iota_L(x) = 1$. Decomposed into the individual components with respect to $\mathcal{T}$, this yields $\partial(\varphi_L(x)_{\mathcal{T}}) \wedge_L \iota_L(x)_{\mathcal{T}} = 1$ and $\partial(\varphi_L(x)_{[i]}) \wedge_L \iota_L(x)_{[i]} = 1$ for $i = 1, \ldots, m$.

One has $\inf(x) = p = \min\{\inf(x_{\mathcal{T}}), \inf(x_{[1]}), \ldots, \inf(x_{[m]})\}$ and, similarly, $\sup(x) = q = \max\{\sup(x_{\mathcal{T}}), \sup(x_{[1]}), \ldots, \sup(x_{[m]})\}$ [4,23]. Moreover, the components of $\iota_L(x)$ and $\varphi_L(x)$ are as follows.

$$\iota_L(x)_{\mathcal{T}} = \begin{cases} \iota_L(x_{\mathcal{T}}); & \inf(x_{\mathcal{T}}) = p \\ \Delta_m \in B_m; & \inf(x_{\mathcal{T}}) > p \end{cases} \qquad \iota_L(x)_{[i]} = \begin{cases} \iota_L(x_{[i]}); & \inf(x_{[i]}) = p \\ \Delta_{k_i} \in B_{k_i}; & \inf(x_{[i]}) > p \end{cases}$$

$$\varphi_L(x)_{\mathcal{T}} = \begin{cases} \varphi_L(x_{\mathcal{T}}); & \sup(x_{\mathcal{T}}) = q \\ 1; & \sup(x_{\mathcal{T}}) < q \end{cases} \qquad \varphi_L(x)_{[i]} = \begin{cases} \varphi_L(x_{[i]}); & \sup(x_{[i]}) = q \\ 1; & \sup(x_{[i]}) < q. \end{cases}$$

Now consider the external component and recall that $\partial(\varphi_L(x)_{\mathcal{T}}) \wedge_L \iota_L(x)_{\mathcal{T}} = 1$. If $\inf(x_{\mathcal{T}}) > p$, that is, $\iota_L(x)_{\mathcal{T}} = \Delta_m$, this implies $\varphi_L(x)_{\mathcal{T}} = \Delta_m$, that is, $x_{\mathcal{T}} = \Delta_m^q$. Similarly, if $\sup(x_{\mathcal{T}}) < q$, that is, $\varphi_L(x)_{\mathcal{T}} = 1$, we obtain $\iota_L(x)_{\mathcal{T}} = 1$, that is, $x_{\mathcal{T}} = \Delta_m^p$. Hence, $x_{\mathcal{T}}$ is either Δ_m^p, or it is Δ_m^q, or it is left rigid with infimum p and supremum q. Observe that in the first case we have $\iota_R(x)_{\mathcal{T}} = 1$, in the second case we have $\iota_R(x)_{\mathcal{T}} = \Delta_m$, and in the third case we have $\iota_R(x)_{\mathcal{T}} = \iota_R(x_{\mathcal{T}})$. Hence, in any case $x_{\mathcal{T}}^{\iota_R(x)_{\mathcal{T}}^{-1}} = \mathbf{c}_R(x_{\mathcal{T}})$, that is, right cycling of x induces right cycling of $x_{\mathcal{T}}$. Similarly, left cycling of x induces left cycling of $x_{\mathcal{T}}$ and left (resp. right) decycling of x induces left (resp. right) decycling of $x_{\mathcal{T}}$. Applying this argument repeatedly, we see that $y \in \mathrm{USS}_R(x)$ implies $y_{\mathcal{T}'} \in \mathrm{USS}_R(x_{\mathcal{T}})$.

Moreover, if $x_{\mathcal{T}} = \Delta_m^p$ or $x_{\mathcal{T}} = \Delta_m^q$ then $y_{\mathcal{T}'} = \mathbf{c}_R^K(x_{\mathcal{T}}) = x_{\mathcal{T}}$ and we have $\partial^{-1}(\varphi_R(y)_{\mathcal{T}'}) \wedge_R \iota_R(y)_{\mathcal{T}'} = 1$. Otherwise, $x_{\mathcal{T}}$ is left rigid with $\ell(x_{\mathcal{T}}) > 1$ and hence (as $x_{\mathcal{T}}$ has fewer strands than x) by induction conjugate to a right rigid braid. By Theorem 2.7 this implies that $y_{\mathcal{T}'} \in \mathrm{USS}_R(x_{\mathcal{T}})$ is right rigid. Hence, in each of the possible cases we have $\partial^{-1}(\varphi_R(y)_{\mathcal{T}'}) \wedge_R \iota_R(y)_{\mathcal{T}'} = 1$.

Following an identical argument for each of the internal components, we obtain $\partial^{-1}(\varphi_R(y)_{[i]}) \wedge_R \iota_R(y)_{[i]} = 1$ for $i = 1, \ldots, m$. Together this implies $\partial^{-1}(\varphi_R(y)) \wedge_R \iota_R(y) = 1$, that is, y is right rigid as we wanted to show. □

4.2. Left and right ultra summit graphs are isomorphic

We will now show that given a left rigid braid $x \in \mathrm{USS}_L(x)$ with $\ell(x) > 1$, the directed graphs $\mathrm{USG}_L(x)$ and $\mathrm{USG}_R(x)$ are isomorphic, with the arrows reversed, that is, we will show Theorem 1.3. We need to define an isomorphism of directed graphs (in other words, an invertible functor from the category $\mathrm{USG}_L(x)$ to the category $\mathrm{USG}_R(x)^{op}$). The isomorphism is very easy to define at the level of vertices (objects), that is, the elements of the ultra summit sets.

Definition 4.9. Let $x \in B_n$ be a left rigid braid, with $\ell(x) = r > 1$. We define $\Phi(x) = \mathbf{c}_R^{2rt}(x)$, where t is any non-negative integer such that $\mathbf{c}_R^{2rt}(x)$ is right rigid.

Notice that Φ is well defined: Since x is left rigid, $x \in \mathrm{SSS}(x)$, so one can go from x to $\mathrm{USS}_R(x)$ by iterated right cycling. Since $\ell(x) > 1$, Theorem 4.8 tells us that x is conjugate to a right rigid element, hence $\mathrm{USS}_R(x)$ consists

of right rigid elements, and one obtains a right rigid element by applying iterated right cycling to x. Also, for every right rigid element z with $\ell(z) = r$, one has $\mathbf{c}_R^{2r}(z) = z$. Hence, if t is an integer such that $\mathbf{c}_R^{2rt}(x)$ is right rigid, then $\mathbf{c}_R^{2rt}(x) = \mathbf{c}_R^{2r}(\mathbf{c}_R^{2rt}(x)) = \mathbf{c}_R^{2r(t+1)}(x)$. This implies that if $\mathbf{c}_R^{2rt}(x)$ and $\mathbf{c}_R^{2rt'}(x)$ are both right rigid, they are equal. Hence Φ is well defined.

We will show below that Φ is a bijective map from $\mathrm{USS}_L(x)$ to $\mathrm{USS}_R(x)$. But we also want to show that $\mathrm{USG}_L(x)$ is isomorphic to $\mathrm{USG}_R(x)^{op}$. We already know a map Φ that sends vertices (objects) of $\mathrm{USG}_L(x)$ to vertices (objects) of $\mathrm{USG}_R(x)^{op}$. Let us see how Φ is defined on the arrows (morphisms) of $\mathrm{USG}_L(x)$. In order to do this, we recall the definition of the transport map. This map is defined in [18] using left normal forms, but, by symmetry, it can equally be defined using right normal forms.

Definition 4.10 (*[18]*). Given an element x of a Garside group G such that $x \in \mathrm{SSS}(x)$ and an element $u \in G$ such that $u^{-1}xu = y \in \mathrm{SSS}(x)$, one defines the **left transport** of u as:

$$u_L^{(1)} = \iota_L(x)^{-1} \cdot u \cdot \iota_L(y).$$

The **iterated left transports** of u are defined recursively, for every $i > 1$, by

$$u_L^{(i)} = \left(u_L^{(i-1)}\right)_L^{(1)}.$$

Notice that, since $u^{-1}xu = y$, one has $\left(u_L^{(i)}\right)^{-1} \mathbf{c}_L^i(x)\ u_L^{(i)} = \mathbf{c}_L^i(y)$. In other words, since u conjugates (on the right) x to y, the ith left transport of u conjugates (on the right) the ith left cycling of x to the ith left cycling of y.

Definition 4.11 (*[18]*). Given an element x of a Garside group G such that $x \in \mathrm{SSS}(x)$ and an element $v \in G$ such that $vxv^{-1} = z \in \mathrm{SSS}(x)$, one defines the **right transport** of v as:

$$v_R^{(1)} = \iota_R(z) \cdot v \cdot \iota_R(x)^{-1}.$$

The **iterated right transports** of v are defined recursively, for every $i > 1$, by

$$v_R^{(i)} = \left(v_R^{(i-1)}\right)_R^{(1)}.$$

As $vxv^{-1} = z$, we have in this case $v_R^{(i)}\, \mathbf{c}_R^i(x) \left(v_R^{(i)}\right)^{-1} = \mathbf{c}_R^i(z)$. In other words, since v conjugates (on the left) x to z, the ith right transport of v conjugates (on the left) the ith right cycling of x to the ith right cycling of z.

Theorem 4.12 (*[18]*). *With the above conditions, one has the following properties, for every $i \geq 1$:*

(1)	*If* $u_1 \preccurlyeq u_2$ *then* $(u_1)_L^{(i)} \preccurlyeq (u_2)_L^{(i)}$.	*If* $v_1 \succcurlyeq v_2$ *then* $(v_1)_R^{(i)} \succcurlyeq (v_2)_R^{(i)}$.
(2)	$(u_1 \wedge_L u_2)_L^{(i)} = (u_1)_L^{(i)} \wedge_L (u_2)_L^{(i)}$.	$(v_1 \wedge_R v_2)_R^{(i)} = (v_1)_R^{(i)} \wedge_R (v_2)_R^{(i)}$.
(3)	$\Delta_L^{(i)} = \Delta$, $\quad 1_L^{(i)} = 1$.	$\Delta_R^{(i)} = \Delta$, $\quad 1_R^{(i)} = 1$.
(4)	*If* u *is simple,* $u_L^{(i)}$ *is simple.*	*If* v *is simple,* $v_R^{(i)}$ *is simple.*
(5)	$(u_1u_2)_L^{(i)} = (u_1)_L^{(i)}(u_2)_L^{(i)}$.	$(v_1v_2)_R^{(i)} = (v_1)_R^{(i)}(v_2)_R^{(i)}$.

Let us then define Φ on the arrows of $\mathrm{USG}_L(x)$.

Definition 4.13. Let $x, y \in \mathrm{USS}_L(x) \subset B_n$ be left rigid braids with $\ell(x) > 1$, and let t be a non-negative integer such that $\Phi(x) = \mathbf{c}_R^{2rt}(x)$ and $\Phi(y) = \mathbf{c}_R^{2rt}(y)$. Given $u \in B_n$ such that $u^{-1}xu = y$, so that $uyu^{-1} = x$, we define $\Phi(u) = u_R^{(2rt)}$.

Proposition 4.14. *Φ is a well-defined map of directed graphs (a well-defined functor) from* $\mathrm{USG}_L(x)$ *to* $\mathrm{USG}_R(x)^{op}$.

Proof. We already know that $\Phi(y) \in \mathrm{USS}_R(x)$ for every $y \in \mathrm{USS}_L(x)$, hence Φ sends vertices of $\mathrm{USG}_L(x)$ to vertices of $\mathrm{USG}_R(x)^{op}$. Now consider an arrow s going from x to y in $\mathrm{USG}_L(x)$, let $p = \inf(x) = \inf(y)$ and let $r = \ell(x) = \ell(y)$. Since $s^{-1}xs = y$, one has $sys^{-1} = x$. Hence, if we define $s_0 = s_R^{(2rt)}$, where t is an integer such that $\Phi(x) = \mathbf{c}_R^{2rt}(x)$ and $\Phi(y) = \mathbf{c}_R^{2rt}(y)$, we have $s_0\,\mathbf{c}_R^{2rt}(y)\,s_0^{-1} = \mathbf{c}_R^{2rt}(x)$, that is, $s_0\,\Phi(y)\,s_0^{-1} = \Phi(x)$, where $\Phi(y)$ and $\Phi(x)$ are right rigid.

In order to be able to define $\Phi(s) = s_0$, we need to show that s_0 does not depend on the choice of the integer t. As $\Phi(y)$ is right rigid and has canonical length r, we have $\mathbf{c}_R^{2r}(\Phi(y)) = \Phi(y)$ and the product of the (left) conjugating elements for $2r$-fold right cycling of $\Phi(y)$ is $\Delta^{-2p}\Phi(y)^2$. In the same way, $\mathbf{c}_R^{2r}(\Phi(x)) = \Phi(x)$ and the product of the (left) conjugating elements for $2r$-fold right cycling of $\Phi(x)$ is $\Delta^{-2p}\Phi(x)^2$. So, the $2r$th iterated right transport of s_0 is $(s_0)_R^{(2r)} = \Delta^{-2p}\Phi(x)^2 s_0 \Phi(y)^{-2}\Delta^{2p} = \Phi(x)^2 s_0 \Phi(y)^{-2} = \Phi(x) s_0 \Phi(y)^{-1} = s_0$, which means that $s_R^{(2rt')} = s_R^{(2rt)} = s_0$ for every $t' \geq t$. Hence $\Phi(s) = s_0$ is a well-defined simple element which is, by the above argument, an arrow in $\mathrm{USG}_R(x)$ going from $\Phi(y)$ to $\Phi(x)$, hence an arrow in $\mathrm{USG}_R(x)^{op}$ going from $\Phi(x)$ to $\Phi(y)$. □

It remains to show that Φ is invertible. In order to do this, we start by recalling a result from [6] that relates cyclings and powers. Given x in a Garside group G, let $C_i = \iota_L(\mathbf{c}_L^{i-1}(x))$ for every $i \geq 1$. That is, C_i is the conjugating element from $\mathbf{c}_L^{i-1}(x)$ to $\mathbf{c}_L^{i}(x)$, and $x^{C_1\cdots C_i} = \mathbf{c}_L^{i}(x)$. Then one has:

Lemma 4.15 (*[6, Lemma 2.4]*). *Let G be a Garside group and let $x \in G$ such that $x \in \mathrm{SSS}(x)$ and $\ell(x) > 1$. Let $p = \inf(x)$. Then, for every $m \geq 1$,*

$$x^m \Delta^{-mp} = C_1 \cdots C_m \mathbf{R}_m,$$

where

(1) $\sup(C_1 \cdots C_m) = m$ *and* $\varphi_L(C_1 \cdots C_m) \succcurlyeq \varphi_L(\mathbf{c}_L^m(x))$.
(2) $\inf(\mathbf{R}_m) = 0$ *and* $\iota_L(\mathbf{R}_m) \preccurlyeq C_{m+1} = \iota_L(\mathbf{c}_L^m(x))$.

This result can be improved if x is conjugate to a left rigid element.

Lemma 4.16. *Let G be a Garside group and let $x \in G$ such that $x \in \mathrm{SSS}(x)$ and $\ell(x) > 1$. Let $p = \inf(x)$. Suppose that x is conjugate to a left rigid element and let m be such that $y = \mathbf{c}_L^m(x)$ is left rigid. Then*

$$C_1 \cdots C_m = (x^m \Delta^{-mp}) \wedge_L \Delta^m,$$

where $\inf(C_1 \cdots C_m) = 0$ *and* $\sup(C_1 \cdots C_m) = m$.

Proof. By the above lemma, $C_1 \cdots C_m \preccurlyeq x^m \Delta^{-mp}$. But since x is conjugate to a rigid element, Lemma 4.2 implies that $\inf(x^m) = mp$, so $\inf(x^m \Delta^{-mp}) = 0$, that is, $\inf(C_1 \cdots C_m) = 0$.

Also, $x^m \Delta^{-pm} = C_1 \cdots C_m \mathbf{R}_m$, where $\varphi_L(C_1 \cdots C_m) \succcurlyeq \varphi_L(\mathbf{c}^m(x)) = \varphi_L(y)$ and $\iota_L(\mathbf{R}_m) \preccurlyeq \iota_L(\mathbf{c}^m(x)) = \iota_L(y)$. Since y is left rigid, the decomposition $\varphi_L(y)\iota_L(y)$ is left-weighted. Hence, if $z_1 \cdots z_m$ is the left normal form of $C_1 \cdots C_m$, this means that $z_1 \cdots z_m \iota_L(\mathbf{R}_m)$ is in left normal form as written. In other words, the first m factors of the left normal form of $x^m \Delta^{-mp}$ are precisely $z_1 \cdots z_m = C_1 \cdots C_m$. That is, $C_1 \cdots C_m = (x^m \Delta^{-mp}) \wedge_L \Delta^m$, as we wanted to show. □

This allows us to determine very precisely the left normal form of x^m, for m big enough, when x is conjugate to a left rigid element. In order to avoid confusing notation produced by the powers of Δ in the normal forms, we will introduce the following notions:

Definition 4.17. Let G be a Garside group. Given an element $z \in G$, whose left normal form is $\Delta^p z_1 \cdots z_r$ and whose right normal form is $z'_1 \cdots z'_r \Delta^p$, we define the **left interior** of z as

$$z_L^\circ = z\Delta^{-p} = \tau^{-p}(z_1) \cdots \tau^{-p}(z_r) = z'_1 \cdots z'_r,$$

and the **right interior** of z as

$$z_R^\circ = \Delta^{-p} z = z_1 \cdots z_r = \tau^p(z'_1) \cdots \tau^p(z'_r).$$

Notice that the above factorisations are, respectively, the left and right normal forms of z_L° and of z_R°. Notice also that if $y = \Delta^p y_1 \cdots y_r$ is left rigid and in left normal form as written, then

$$(y^m)_L^\circ = y^m \Delta^{-pm} = \left(\tau^{-p}(y_1) \cdots \tau^{-p}(y_r)\right) \cdot \left(\tau^{-2p}(y_1) \cdots \tau^{-2p}(y_r)\right) \cdots \left(\tau^{-mp}(y_1) \cdots \tau^{-mp}(y_r)\right),$$

and the latter expression is in left normal form as written. Moreover, in this case $(y^m)_L^\circ$ is precisely the conjugating element that takes y to $\mathbf{c}_L^{rm}(y)$. Similarly, if $y = y_1 \cdots y_r \Delta^p$ is right rigid and in right normal form as written, then

$$(y^m)_R^\circ = \Delta^{-pm} y^m = \left(\tau^{mp}(y_1) \cdots \tau^{mp}(y_r)\right) \cdots \left(\tau^{2p}(y_1) \cdots \tau^{2p}(y_r)\right) \cdot \left(\tau^{p}(y_1) \cdots \tau^{p}(y_r)\right),$$

and the latter expression is in right normal form as written. Moreover, in this case $(y^m)_R^\circ$ is precisely the (left) conjugating element that takes y to $\mathbf{c}_R^{rm}(y)$.

Lemma 4.18. *Let G be a Garside group and let $x \in G$ such that $x \in \mathrm{SSS}(x)$ and $\ell(x) = r > 1$. Let $p = \inf(x)$. Suppose that x is conjugate to a left rigid element and let N be such that $y = \mathbf{c}_L^N(x)$ is left rigid. Then the following hold:*

(1) *For any integer $M \geq N$, one has $\left(y^M\right)_R^\circ \succcurlyeq C_1 \cdots C_N$.*
(2) *Let M be an integer satisfying the condition $\left(y^M\right)_R^\circ \succcurlyeq C_1 \cdots C_N$. If $z_1 \cdots z_N$ is the left normal form of $C_1 \cdots C_N$, and $z'_1 \cdots z'_s$ is the left normal form of $\left(y^M\right)_R^\circ (C_1 \cdots C_N)^{-1}$, then for every $m \geq M$, the left normal form of $(x^m)_L^\circ$ is*

$$(x^m)_L^\circ = (z_1 \cdots z_N) \cdot \left(y^{m-M}\right)_L^\circ \cdot \left(\tau^{-pm}(z'_1) \cdots \tau^{-pm}(z'_s)\right),$$

where the middle factor is assumed to be written in left normal form. Moreover, $N + s = Mr$.

Proof. Recall that $x^{C_1 \cdots C_N} = \mathbf{c}_L^N(x) = y$, so $\left(x^N\right)^{C_1 \cdots C_N} = y^N$. Recall also that by Lemma 4.16 one has $C_1 \cdots C_N \preccurlyeq x^N \Delta^{-pN} = \left(x^N\right)_L^\circ$. This means that $\alpha = (C_1 \cdots C_N)^{-1} \left(x^N\right)_L^\circ$ is a positive braid. Now,

$$\begin{aligned} y^N &= (C_1 \cdots C_N)^{-1} x^N (C_1 \cdots C_N) \\ &= \alpha \Delta^{pN} C_1 \cdots C_N = \Delta^{pN} \tau^{pN}(\alpha) C_1 \cdots C_N, \end{aligned}$$

and thus $\left(y^M\right)_R^\circ \succcurlyeq \left(y^N\right)_R^\circ = \Delta^{-pN} y^N = \tau^{pN}(\alpha) C_1 \cdots C_N \succcurlyeq C_1 \cdots C_N$. Hence the first claim is shown.

Now let M, m, $z_1 \cdots z_N$ and $z'_1 \cdots z'_s$ be defined as in claim (2). Notice that since $m \geq M$, one has $(y^m)_R^\circ = \Delta^{-pm} y^m \succcurlyeq \Delta^{-pM} y^M \succcurlyeq C_1 \cdots C_N$. That is, there exists a positive braid β such that $y^m = \Delta^{mp} \beta C_1 \cdots C_N$. By Lemma 4.15, $\varphi_L(C_1 \cdots C_N) \succcurlyeq \varphi_L(\mathbf{c}_L^N(x)) = \varphi_L(y)$. Also, $\iota_L(\tau^{-mp}(\beta)) \preccurlyeq \iota_L(y^m) = \iota_L(y)$, where the last equality follows from the rigidity of y. As $\varphi_L(y)\iota_L(y)$ is left-weighted, this implies that $z_N \iota_L(\tau^{-mp}(\beta))$ is also left-weighted.

Observe that

$$\begin{aligned} x^m &= (C_1 \cdots C_N) \cdot y^m \cdot (C_1 \cdots C_N)^{-1} \\ &= C_1 \cdots C_N \Delta^{mp} \beta = C_1 \cdots C_N \tau^{-mp}(\beta) \Delta^{mp}, \end{aligned}$$

whence $(x^m)_L^\circ = C_1 \cdots C_N \tau^{-mp}(\beta) = z_1 \cdots z_N \tau^{-mp}(\beta)$. Since $z_N \iota_L(\tau^{-mp}(\beta))$ is left-weighted, it follows that the first N factors in the left normal form of $(x^m)_L^\circ$ are precisely $z_1 \cdots z_N$.

Now recall that $z'_1 \cdots z'_s$ is the left normal form of $\Delta^{-pM} y^M (C_1 \cdots C_N)^{-1}$. Hence

$$\begin{aligned} y^m &= y^{m-M} y^M = \left(y^{m-M}\right)_L^\circ \Delta^{p(m-M)} \Delta^{pM} z'_1 \cdots z'_s C_1 \cdots C_N \\ &= \left(y^{m-M}\right)_L^\circ \Delta^{pm} z'_1 \cdots z'_s C_1 \cdots C_N \\ &= \left(y^{m-M}\right)_L^\circ \left(\tau^{-pm}(z'_1) \cdots \tau^{-pm}(z'_s)\right) \Delta^{pm} C_1 \cdots C_N. \end{aligned}$$

Conjugating by $(C_1 \cdots C_N)^{-1}$, one obtains

$$x^m = (C_1 \cdots C_N) \left(y^{m-M}\right)_L^\circ \left(\tau^{-pm}(z'_1) \cdots \tau^{-pm}(z'_s)\right) \Delta^{pm},$$

hence

$$(x^m)^\circ_L = (z_1 \cdots z_N) \cdot \left(y^{m-M}\right)^\circ_L \cdot \left(\tau^{-pm}(z'_1) \cdots \tau^{-pm}(z'_s)\right).$$

This is written in left normal form, as $\varphi_L\left(\left(y^{m-M}\right)^\circ_L\right) \tau^{-pm}(z'_1)$ is left-weighted. The latter can be seen by noticing that $\varphi_L\left(\left(y^{m-M}\right)^\circ_L\right) = \varphi_L\left(\tau^{-p(m-M)}(y)\right)$ and that moreover $z'_1 = \iota_L\left(\Delta^{-pM} y^M (C_1 \cdots C_N)^{-1}\right) \preccurlyeq \iota_L\left(\tau^{pM}(y)\right)$, whence $\tau^{-pm}(z'_1) \preccurlyeq \iota_L\left(\tau^{-p(m-M)}(y)\right)$.

Finally, the left rigidity of y implies that x is periodically geodesic, whence $\ell(x^m) = \ell\left((x^m)^\circ_L\right) = mr$. But we just computed the left normal form of $(x^m)^\circ_L$, which has $N + (m-M)r + s$ factors. Therefore $N + (m-M)r + s = mr$, so $N + s = Mr$, as we wanted to show. □

By symmetry, one has the analogous result for conjugates of right rigid braids, but we will perform a slight modification:

Lemma 4.19. *Let G be a Garside group and let $x \in G$ such that $x \in \mathrm{SSS}(x)$ and $\ell(x) = r > 1$. Let $p = \inf(x)$. Suppose that x is conjugate to a right rigid element and let N be such that $y = \mathbf{c}_R^N(x)$ is right rigid. Let $C'_1, \ldots, C'_N$ be the (left) conjugating elements for the N iterated right cyclings of y, that is, $(C'_N \cdots C'_1)\, x\, (C'_N \cdots C'_1)^{-1} = y$. Then the following hold:*

(1) *For any integer $M \geq N$, one has $C'_N \cdots C'_1 \preccurlyeq \left(y^M\right)^\circ_L$.*
(2) *Let e be a positive integer such that Δ^e is central in G and let M be a multiple of e, such that $C'_N \cdots C'_1 \preccurlyeq \left(y^M\right)^\circ_L$. In this case, if $z'_N \cdots z'_1$ is the right normal form of $C'_N \cdots C'_1$ and $z_s \cdots z_1$ is the right normal form of $(C'_N \cdots C'_1)^{-1}\left(y^M\right)^\circ_L$, then for every $m \geq M$, the right normal form of $(x^m)^\circ_L$ is*

$$(x^m)^\circ_L = (z_s \cdots z_1) \cdot \left(y^{m-M}\right)^\circ_L \cdot \left(\tau^{-pm}(z'_N) \cdots \tau^{-pm}(z'_1)\right),$$

where the middle factor is assumed to be written in right normal form. Moreover, $N + s = Mr$.

Proof. If one follows the argument of Lemma 4.18 for right normal forms, one obtains that the right normal form of $(x^m)^\circ_R$ is

$$(x^m)^\circ_R = \left(\tau^{pm}(z_s) \cdots \tau^{pm}(z_1)\right) \cdot \left(y^{m-M}\right)^\circ_R \cdot \left(z'_N \cdots z'_1\right),$$

and now one just has to notice that $(x^m)^\circ_L = \tau^{-mp}\left((x^m)^\circ_R\right)$ and that, since M is a multiple of e and hence τ^M is the identity,

$$\tau^{-pm}\left(\left(y^{m-M}\right)^\circ_R\right) = \tau^{-p(m-M)}\left(\left(y^{m-M}\right)^\circ_R\right) = \left(y^{m-M}\right)^\circ_L. \quad \square$$

We can now show that Φ is a bijective map on the vertices.

Proposition 4.20. *Let $x \in B_n$ be a left rigid braid with $\ell(x) > 1$. The map $\Phi : \mathrm{USS}_L(x) \to \mathrm{USS}_R(x)$ defined above is bijective.*

Proof. Recall the involutory anti-isomorphism $\mathrm{rev} : B_n \to B_n$ introduced in Section 2, which sends a braid $x = \sigma_{i_1}^{e_1} \cdots \sigma_{i_m}^{e_m}$ to its reverse $\mathrm{rev}(x) = \overleftarrow{x} = \sigma_{i_m}^{e_m} \cdots \sigma_{i_1}^{e_1}$. We define a map $\Psi : \mathrm{USS}_R(x) \to \mathrm{USS}_L(x)$ as symmetric analogue of Φ under rev, that is, $\Psi(z) = \overleftarrow{\Phi(\overleftarrow{z})}$. We will show that Ψ is the inverse of Φ.

Let $\Delta^p x_1 \cdots x_r$ be the left normal form of x. Recall that $\Phi(x) = \mathbf{c}_R^{2rt}(x)$ for some integer t, and that $\Phi(x) = \mathbf{c}_R^{2rt'}(x)$ for every $t' \geq t$. Similarly, we have $\Psi(\Phi(x)) = \mathbf{c}_L^{2rs}(\Phi(x))$ for some integer s, and then $\Psi(\Phi(x)) = \mathbf{c}_L^{2rs'}(\Phi(x))$ for every $s' \geq s$. Hence, defining $N = 2r\max(t,s)$, we have $\Phi(x) = \mathbf{c}_R^N(x)$ and $\Psi(\Phi(x)) = \mathbf{c}_L^N(\Phi(x)) = \mathbf{c}_L^N(\mathbf{c}_R^N(x))$. We must then show that $\mathbf{c}_L^N(\mathbf{c}_R^N(x)) = x$.

In order to do this, we will study some decompositions of x^m, for m big enough. For simplicity, we will consider m to be even. First, since x is left rigid, the left normal form of $(x^m)^\circ_L$ for every even m is precisely:

$$\begin{aligned}\left(x^m\right)^\circ_L &= \left(\tau^{-p}(x_1) \cdots \tau^{-p}(x_r)\right) \cdot \left(\tau^{-2p}(x_1) \cdots \tau^{-2p}(x_r)\right) \cdots \left(\tau^{-mp}(x_1) \cdots \tau^{-mp}(x_r)\right) \\ &= \left(\tau^{-p}(x_1) \cdots \tau^{-p}(x_r) x_1 \cdots x_r\right)^{m/2} = \left(\left(x^2\right)^\circ_L\right)^{m/2}.\end{aligned}$$

Notice that if p is even, the above expression is just $(x_1 \cdots x_r)^m$, but if p is odd this does not happen in general.

Now x is conjugate to a right rigid braid, $y = \Phi(x)$. We can then apply Lemma 4.19 to x. We fix M as in Lemma 4.19, where we can assume that M is even (otherwise, take $M+1$). We take m big enough, so that $m > 2M$ and m is even. We then obtain that the right normal form of $(x^m)^\circ_L$ is:

$$\begin{aligned}\left(x^m\right)^\circ_L &= (z_s \cdots z_1) \cdot \left(y^{m-M}\right)^\circ_L \cdot \left(\tau^{-pm}(z'_N) \cdots \tau^{-pm}(z'_1)\right)\\ &= (z_s \cdots z_1) \cdot \left(y^{m-M}\right)^\circ_L \cdot \left(z'_N \cdots z'_1\right).\end{aligned}$$

By definition, $(z'_N \cdots z'_1)(z_s \cdots z_1) = (y^M)^\circ_L = y^M \Delta^{-pM}$. Also by definition, $z'_N \cdots z'_1 = C'_N \cdots C'_1$ is the (left) conjugating element for N-fold iterated right cycling of x, that is, $(z'_N \cdots z'_1)\, x\, (z'_N \cdots z'_1)^{-1} = \mathbf{c}^N_R(x) = y$. Hence we have $\left(x^M\right)^\circ_L = x^M \Delta^{-pM} = (z'_N \cdots z'_1)^{-1} y^M \Delta^{-pM} (z'_N \cdots z'_1) = (z_s \cdots z_1)(z'_N \cdots z'_1)$. Note that we used that M is even, by assuming Δ^{pM} to be central.

As x is left rigid and both m and M are even, we then obtain the following decomposition:

$$\begin{aligned}(x^m)^\circ_L &= (x^M)^\circ_L (x^{m-2M})^\circ_L (x^M)^\circ_L\\ &= (z_s \cdots z_1)\left(z'_N \cdots z'_1\right) \cdot \left(x^{m-2M}\right)^\circ_L \cdot (z_s \cdots z_1)\left(z'_N \cdots z'_1\right),\end{aligned}$$

whence

$$\left(y^{m-M}\right)^\circ_L = \left(z'_N \cdots z'_1\right) \cdot \left(x^{m-2M}\right)^\circ_L \cdot (z_s \cdots z_1).$$

Let us write the above factors in left normal form: Let $w_1 \cdots w_N$ be the left normal form of $z'_N \cdots z'_1$, and let $w'_1 \cdots w'_s$ be the left normal form of $z_s \cdots z_1$. Then

$$\left(y^{m-M}\right)^\circ_L = (w_1 \cdots w_N) \cdot \left(x^{m-2M}\right)^\circ_L \cdot \left(w'_1 \cdots w'_s\right).$$

We will now show that this decomposition is precisely the left normal form of $\left(y^{m-M}\right)^\circ_L$. Indeed, as $\left(x^M\right)^\circ_L = (z_s \cdots z_1)(z'_N \cdots z'_1) = \left(w'_1 \cdots w'_s\right)(w_1 \cdots w_N)$ and $s + N = Mr$ by Lemma 4.19, it follows that the final factor of the left normal form of $\left(x^M\right)^\circ_L$ is a suffix of w_N. That is, $w_N \succcurlyeq x_r$. Since x is left rigid, this implies that $w_N \cdot \tau^{-p}(x_1)$ is left-weighted, where the second factor in this expression is the initial factor in the left normal form of $\left(x^{m-2M}\right)^\circ_L$. Moreover, w'_1 must be a prefix of the initial factor of $\left(x^M\right)^\circ_L$, that is, $w'_1 \preccurlyeq \tau^{-p}(x_1)$. This implies that $x_r \cdot w'_1$ is left-weighted, where x_r is the final factor in the left normal form of $\left(x^{m-2M}\right)^\circ_L$. Hence, the above expression is the left normal form of $\left(y^{m-M}\right)^\circ_L$, for even m with $m > 2M$.

Choose now m such that $m - M$ is a multiple of $2r$ and $m - M \geq N$ and consider the product P of the first $m - M$ factors in the left normal form of $\left(y^{m-M}\right)^\circ_L$. By the above argument we have $P = w_1 \cdots w_N \left(x^{2k}\right)^\circ_L$, where $k = \frac{(m-M)-N}{2r}$. (Note that N is a multiple of $2r$, so k is an integer.) However, as $\mathbf{c}^{m-M}_L(y)$ is left rigid, P is the conjugating element for $(m-M)$-fold left cycling of y by Lemma 4.16, and as $\left(x^{2k}\right)^\circ_L = x^{2k}\Delta^{-2kp}$ commutes with x, we obtain

$$\begin{aligned}\mathbf{c}^{m-M}_L(y) = y^P &= \left(\left(x^{2k}\right)^\circ_L\right)^{-1} \cdot (w_1 \cdots w_N)^{-1} \cdot y \cdot (w_1 \cdots w_N) \cdot \left(x^{2k}\right)^\circ_L\\ &= \left(\left(x^{2k}\right)^\circ_L\right)^{-1} \cdot x \cdot \left(x^{2k}\right)^\circ_L = x.\end{aligned}$$

We finally obtain $\Psi(\Phi(x)) = \Psi(y) = \mathbf{c}^{m-M}_L(y) = x$, as we wanted to show. □

In order to finish the proof of Theorem 1.3, it just remains to show that the map Ψ can be extended to the arrows of $\mathrm{USG}_R(x)$, so that $\Psi \circ \Phi = \mathrm{id}_{\mathrm{USG}_L(x)}$. We will use the following result:

Lemma 4.21. *Let $x \in B_n$ be left rigid with $\ell(x) = r > 1$. Let $T = 2rt$ be such that $\Phi(x) = \mathbf{c}^T_R(x)$ and $\Psi(\Phi(x)) = \mathbf{c}^T_L(\Phi(x))$. Let $C'_T, \ldots, C'_1$ be the (left) conjugating elements for the iterated right cyclings of x, and let $C_1, \ldots, C_T$ be the conjugating elements for the iterated left cyclings of $\Phi(x)$. That is,*

$$\Phi(x) = (C'_1 \cdots C'_T)\, x\, (C'_1 \cdots C'_T)^{-1}$$

and

$$\Psi(\Phi(x)) = (C_1 \cdots C_T)^{-1}\, \Phi(x)\, (C_1 \cdots C_T).$$

Then, $C_1 \cdots C_T = C'_1 \cdots C'_T$.

Proof. Using the notation in the proof of Proposition 4.20, we notice that the left normal form of $C_1 \cdots C_T$ is $(w_1 \cdots w_N)(x^{2k})^\circ_L$, where $k = \frac{T-N}{2r}$. Similarly, using the symmetry under rev, the right normal form of $C'_1 \cdots C'_T$ is $(y^{2k})^\circ_R(z'_N \cdots z'_1) = (y^{2k})^\circ_L(z'_N \cdots z'_1)$ for the same value of k. (Note that $\sup(C_1 \cdots C_T) = T = \sup(C'_1 \cdots C'_T)$ and that τ^{2kp} is trivial.) As, moreover, $(y^{2k})^\circ_L(z'_N \cdots z'_1) = (z'_N \cdots z'_1)(x^{2k})^\circ_L = (w_1 \cdots w_N)(x^{2k})^\circ_L$, by definition of $z'_N, \ldots, z'_1$ and $w_1, \ldots, w_N$, respectively, the result follows. □

Proof of Theorem 1.3. We define $\Psi : \mathrm{USG}_R(x)^{op} \to \mathrm{USG}_L(x)$ in the natural way. For every element $u \in \mathrm{USS}_R(x)$, we define $\Psi(u)$ as above, in the same way as Φ but using right normal forms, that is, $\Psi(u) = \overleftarrow{\Phi(\overleftarrow{u})}$. In the case of the arrows of $\mathrm{USG}_R(x)^{op}$, we proceed exactly the same way. If s is a simple element such that $sus^{-1} = v$ with $u, v \in \mathrm{USS}_R(x)$, that is, if s is an arrow in $\mathrm{USG}_R(x)^{op}$ going from v to u, we define $\Psi(s) = \overleftarrow{\Phi(\overleftarrow{s})}$, where $\overleftarrow{s}$ corresponds to an arrow in $\mathrm{USG}_L(\overleftarrow{x})$ going from $\overleftarrow{u}$ to $\overleftarrow{v}$.

Let us show that, if s is an arrow in $\mathrm{USG}_L(x)$ going from x to y, then $\Psi(\Phi(s)) = s$. First, by construction, $\Psi(\Phi(s))$ is a simple element conjugating $\Psi(\Phi(x)) = x$ to $\Psi(\Phi(y)) = y$, hence $\Psi(\Phi(s))$ is an arrow in $\mathrm{USG}_L(x)$ going from x to y. We just need to show that s and $\Psi(\Phi(s))$ are the same simple elements.

Let $N = 2rt$ be big enough, so that we have $\Phi(x) = \mathbf{c}^N_R(x)$, $\Phi(y) = \mathbf{c}^N_R(y)$, $\Psi(\Phi(x)) = \mathbf{c}^N_L(\Phi(x))$ and $\Psi(\Phi(y)) = \mathbf{c}^N_L(\Phi(y))$. By Lemma 4.21, the product of the conjugating elements (on the left) leading from x to $\Phi(x)$ equals the product of the conjugating elements (on the right) leading from $\Phi(x)$ to $\Psi(\Phi(x)) = x$; we denote this product by α. The same situation occurs for y and $\Phi(y)$; we denote the corresponding product by β. Finally, we obtain $\Psi(\Phi(s)) = \Psi(s^{(N)}_R) = \Psi(\alpha s \beta^{-1}) = \alpha^{-1}(\alpha s \beta^{-1})\beta = s$ as claimed. □

We remark that, since the left (resp. right) transport preserves left (resp. right) gcds by Theorem 4.12, Φ sends minimal arrows of $\mathrm{USG}_L(x)$ to minimal arrows of $\mathrm{USG}_R(x)^{op}$ and Ψ sends minimal arrows in $\mathrm{USG}_R(x)^{op}$ to minimal arrows of $\mathrm{USG}_L(x)$. Therefore, we have:

Corollary 4.22. *Let $x \in B_n$ be left rigid with canonical length $\ell(x) > 1$. The restriction of Φ to* $\mathrm{minUSG}_L(x)$ *is an isomorphism of directed graphs:* $\Phi : \mathrm{minUSG}_L(x) \to \mathrm{minUSG}_R(x)^{op}$.

4.2.1. Φ respects the structure of ultra summit graphs

It was shown in [7] that the arrows of $\mathrm{minUSG}_L(x)$, and similarly those of $\mathrm{minUSG}_R(x)$, can be grouped naturally into two classes, namely *partial cycling* and *partial twisted decycling* components. In this subsection we show that the isomorphism Φ is natural in the sense that it preserves this decomposition of ultra summit graphs.

Proposition 4.23 (*[7]*). *Let x be an element of a Garside group with $\ell(x) > 0$ and let s be an arrow in* $\min \mathrm{USG}_L(x)$ *going from x to $x^s = s^{-1}xs$. Then at least one of the following conditions holds:*

(1) $s \preccurlyeq \iota_L(x)$
(2) $s \preccurlyeq \iota_L(x^{-1})$.

If x is left rigid, then exactly one of the above conditions holds.

Notice that $\iota_L(x^{-1}) = \partial(\varphi_L(x))$.

Definition 4.24 (*[7]*). Let x be an element of a Garside group with $\ell(x) > 0$ and let s be an arrow in $\mathrm{USG}_L(x)$ going from x to $x^s = s^{-1}xs$. If $s \preccurlyeq \iota_L(x)$, we call s a **partial left cycling** of x and say that the arrow s is **black**. If $s \preccurlyeq \iota_L(x^{-1}) = \partial(\varphi_L(x))$, we call s a **partial twisted left decycling** of x and say that the arrow s is **grey**.

By symmetry we have:

Proposition 4.25 (*[7]*). *Let x be an element of a Garside group with $\ell(x) > 0$ and let s be an arrow in* $\min \mathrm{USG}_R(x)$ *going from x to sxs^{-1}. Then at least one of the following conditions holds:*

(1) $\iota_R(x) \succcurlyeq s$
(2) $\iota_R(x^{-1}) \succcurlyeq s$.

If x is right rigid, then exactly one of the above conditions holds.

Notice that $\iota_R(x^{-1}) = \partial^{-1}(\varphi_R(x))$.

Definition 4.26 (*[7]*). Let x be an element of a Garside group with $\ell(x) > 0$ and let s be an arrow in $\mathrm{USG}_R(x)$ going from x to sxs^{-1}. If $\iota_R(x) \succcurlyeq s$, we call s a **partial right cycling** of x and say that the arrow s is **black**. If $\partial^{-1}(\varphi_R(x)) = \iota_R(x^{-1}) \succcurlyeq s$, we call s a **partial twisted right decycling** of x and say that the arrow s is **grey**.

Note that the intuitive meaning of "cycling" (respectively "decycling") is to move the first simple factor to the end (respectively, the last simple factor to the front) with respect to the normal form under consideration. Note, moreover, that $\tau \circ \mathbf{d}_L(x) = \tau(x^{\varphi_L(x)^{-1}}) = \tau(x^{\iota_L(x^{-1})\Delta^{-1}}) = x^{\iota_L(x^{-1})}$ and that, analogously, $\tau^{-1} \circ \mathbf{d}_R(x) = \tau^{-1}(x^{\varphi_R(x)}) = \tau^{-1}(x^{\iota_R(x^{-1})^{-1}\Delta}) = x^{\iota_R(x^{-1})^{-1}}$. Hence, the definitions of "partial cycling" and "partial twisted decycling" are natural: a *partial* cycling or decycling corresponds to moving *a prefix* or *a suffix* of the first or last simple factor; "twisting" refers to composition with τ.

Partial cyclings and partial twisted decyclings are preserved by the graph isomorphism Φ according to the following results.

Proposition 4.27. *Let $x \in B_n$ be a left rigid braid with $\ell(x) = r > 1$ and let s be an arrow from x to y in $\mathrm{USG}_L(x)$ such that $s \preccurlyeq \iota_L(x)$. Then, $\Phi(s)$ is an arrow from $\Phi(y)$ to $\Phi(x)$ in $\mathrm{USG}_R(x)$ such that $\iota_R(\Phi(y)) \succcurlyeq \Phi(s)$.*

Proof. We know that $\Phi(s)$ is an arrow from $\Phi(y)$ to $\Phi(x)$, so what we still need to prove is $\iota_R(\Phi(y)) \succcurlyeq \Phi(s)$. As $\iota_R(\Phi(y)) = \Phi(y)^{\circ}_R \wedge_R \Delta$ and $\Phi(s)$ is simple, it is sufficient to show that $\Phi(y)^{\circ}_R \succcurlyeq \Phi(s)$.

Recall that Φ is defined via iterated right cycling (for vertices), respectively iterated right transport (for arrows). Let N be an integer sufficiently large so that $\Phi(x) = \mathbf{c}_R^{2rN}(x)$ and $\Phi(s) = s_R^{(2rN)}$. Denoting by C the (left) conjugating element for $2rN$-fold right cycling of x, we observe that, by the definition of the right transport, we have $\Phi(x) = \mathbf{c}_R^{2rN}(x) = CxC^{-1} = x_R^{(2rN)}$.

Let $p = \inf(x)$. Since we are assuming $s \preccurlyeq \iota_L(x) \preccurlyeq x^{\circ}_L$, there is a positive braid α, such that $x = s\alpha\Delta^p$, and as the right transport respects products by Theorem 4.12, we obtain $\Phi(x) = x_R^{(2rN)} = s_R^{(2rN)}\alpha_R^{(2rN)}\Delta^p = \Phi(s)\alpha_R^{(2rN)}\Delta^p$, where $\alpha_R^{(2rN)}$ is positive. Hence, $\Phi(s) \preccurlyeq \Phi(x)\Delta^{-p}$, that is, $\Phi(s)^{-1}\Phi(x)\Delta^{-p}$ is positive, which implies that $\Delta^{-p}\Phi(s)^{-1}\Phi(x)$ is positive, too. We finally obtain $\Phi(y)^{\circ}_R = \Delta^{-p}\Phi(y) = \Delta^{-p}\Phi(s)^{-1}\Phi(x)\Phi(s) \succcurlyeq \Phi(s)$ completing the proof. □

Corollary 4.28. *Let $x \in B_n$ be a left rigid braid with $\ell(x) > 1$. Then, Φ and Ψ as defined above are isomorphisms of the directed graphs $\mathrm{USG}_L(x)$ and $\mathrm{USG}_R(x)^{op}$ preserving the colours of arrows.*

Proof. We know that Φ and Ψ are isomorphisms of directed graphs by Theorem 1.3; it remains to be shown that they preserve the colours of arrows.

By Proposition 4.27, the image of a black arrow under Φ is a black arrow. Applying Proposition 4.27 to x^{-1}, which is also a rigid braid with $\ell(x^{-1}) > 1$, it follows that the image of a grey arrow under Φ is a grey arrow. The analogous result holds for Ψ by symmetry. □

Acknowledgements

This paper was conceived in the framework of a collaboration of the authors with Joan S. Birman. Most arguments in it have been discussed with her, and in particular she participated in finding the right conjectures that became Theorems 1.2 and 1.3. We are deeply grateful to her for these contributions, and also for her advice and support. The first author thanks Thierry Berger and Samuel Maffre for inviting him to Limoges, to the PhD defence of the latter, where he learnt about the results which are a key tool in Section 3. We thank the referees for their useful comments on an earlier version of this paper.

The first author was partially supported by MTM2004-07203-C02-01 and FEDER.

References

[1] S.I. Adyan, Fragments of the word Δ in the braid group, Mat. Zametki 36 (1984) 25–34 (in Russian).
[2] I. Anshel, M. Anshel, D. Goldfeld, An algebraic method for public key cryptography, Math. Res. Lett. 6 (1999) 287–291.
[3] E. Artin, Theory of braids, Ann. of Math. 48 (1946) 101–126.
[4] D. Bernardete, M. Gutierrez, Z. Nitecki, Braids and the Nielsen–Thurston classification, J. Knot Theory Ramifications 4 (1995) 549–618.
[5] D. Bessis, The dual braid monoid, Ann. Sci. École Norm. Sup. (4) 36 (2003) 647–683.
[6] J. Birman, V. Gebhardt, J. González-Meneses, Conjugacy in Garside groups I: Cycling, Powers and Rigidity, Groups Geom. Dynam. 1 (2007) 221–279.
[7] J. Birman, V. Gebhardt, J. González-Meneses, Conjugacy in Garside groups II: Structure of the Ultra Summit Set, Groups Geom. Dynam. 2 (2008) 13–61.
[8] J. Birman, V. Gebhardt, J. González-Meneses, Conjugacy in Garside groups III: Periodic braids, J. Algebra 316 (2007) 746–776.
[9] J. Birman, K.Y. Ko, S.J. Lee, A new approach to the word and conjugacy problems in the braid groups, Adv. Math. 139 (1998) 322–353.
[10] J. Birman, A. Lubotzky, J. McCarthy, Abelian and solvable subgroups of the mapping class groups, Duke Math. J. 50 (1983) 1107–1120.
[11] P. Dehornoy, L. Paris, Gaussian groups and Garside groups, two generalizations of Artin groups, Proc. London Math. Soc. 79 (1999) 569–604.
[12] P. Dehornoy, Groupes de Garside, Ann. Sci. École Norm. Sup. 35 (2002) 267–306.
[13] P. Dehornoy, Braid-based cryptography, in: Alexei Myasnikov, Vladimir Shpilrain (Eds.), Group Theory, Statistics and Cryptography, in: Contemporary Mathematics, vol. 360, 2004, pp. 5–33.
[14] P. Deligne, Les immeubles des groupes de tresses generalises, Invent. Math. 17 (1972) 273–302.
[15] E. ElRifai, H. Morton, Algorithms for positive braids, Quart. J. Math. Oxford Ser (2) 45 (1994) 479–497.
[16] D. Epstein, J. Cannon, F. Holt, S. Levy, M. Patterson, W. Thurston, Word Processing in Groups, Jones and Bartlett, Boston, MA, 1992.
[17] F. Garside, The braid group and other groups, Quart. J. Math Oxford 20 (1969) 235–254.
[18] V. Gebhardt, A new approach to the conjugacy problem in Garside groups, J. Algebra 292 (2005) 282–302.
[19] J. González-Meneses, The nth root of a braid is unique up to conjugacy, Algebraic Geom. Topol. 3 (2003) 1103–1118.
[20] K.H. Ko, J.W. Lee, A polynomial-time solution to the reducibility problem, preprint: arXiv math.GT/0610746.
[21] K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J. Kang, C. Park, New public key cryptosystems using braid groups, in: Lecture Notes in Computer Science, vol. 1880, Springer, Berlin, 2000.
[22] E.-K. Lee, S.J. Lee, Translation numbers in a Garside group are rational with uniformly bounded denominators, J. Pure Appl. Algebra 211 (2007) 732–743.
[23] E.-K. Lee, S.J. Lee, A Garside-theoretic approach to the reducibility problem in braid groups, preprint: arXiv math.GT/0506188.
[24] S. Maffre, Ph.D. Thesis, Université de Limoges, 2005. www.unilim.fr/theses/2005/sciences/2005limo0028/maffre_s.pdf.
[25] M. Picantin, Ph.D. Thesis, Université de Caen, 2000. www.liafa.jussieu.fr/ picantin/publi.html.